Universidad Católica Andrés Bello
Dirección de Formación Continua
Urb. La Castellana. Chacao.
Av. Santa Teresa de Jesús. Edificio CERPE.
Teléfonos: 263.76.60/25.82/48.77/
Telefax: 263.95.55

Dirección de Formación Continua

Diploma de Estudios Avanzados en Gestión de las Comunicaciones y Tecnologías de la Información
UCAB

AMERICA Escuela de Organización Industrial de España

Diploma de Estudios Avanzados en
Gestión de las Comunicaciones y Tecnologías de la Información

TESIS
GCTI 2002
B7

Un esquema de Seguridad para un ambiente inseguro
La Universidad

Autor: Pedro Brao F

UN ESQUEMA DE SEGURIDAD PARA UN AMBIENTE INSEGURO LA UNIVERSIDAD

Elaborado por

Pedro Brao F.

Tesis Sometida para cumplir con los requisitos requeridos para optar al

Diplomado de Estudios Avanzados en Gestión de las Comunicaciones y Tecnologías de la Información

Universidad Católica Andrés Bello (UCAB)

2002

Aprobado por: Teodoro Lobo

_____

_____

_____

Universidad Católica Andares Bello

(UCAB)

Abstracto

UN ESQUEMA DE SEGURIDAD PARA UN AMBIENTE INSEGURO LA UNIVERSIDAD

Elaborada por Pedro Brao F.

Por sus propias características, el ámbito universitario quiere desarrollarse en un ambiente de libertad, de facilidades para la investigación, de libre expresión y muy limitada represión. Todo ello constituye un fabuloso reto enmarcar a un usuario que por tradición no ha tenido restricciones, haciéndole comprender que el establecimiento de un orden por demás lógico, no limitara sus libertades.

Objetivo

Investigar la situación actual del ambiente universitario, en el área de Seguridad de Datos, y basándose en ello identificar sus necesidades presentes y futuras sobre la base de sus requerimientos académicos, administrativos y de investigación. A fin de proponer una metodología que permita definir una política de Seguridad de Datos, la aceptación por toda la comunidad, su implantación y finalmente utilizar las enseñanzas obtenidas para hacer posible que usando los recursos del medio universitario logra su comercialización para otros ambientes.

Alcance

El trabajo estará conformado por las siguientes fases

I. **Identificación de necesidades** determinar si los esquemas de Seguridad que viene utilizando la Universidad cubre las expectativas que los diversos elementos de la comunidad universitaria esperan. Determinar si las mismas respetan los principios de confidencialidad, disponibilidad y privacidad, pilares que conforman y sustentan cualquier política de Seguridad de Datos
II. **Propuesta de Política** definir el funcionamiento de las áreas de investigación, administración, académica y administrativa. Sobre la base de ello se definirá y propondrá una política de Seguridad de Información.
III. **Divulgación de la Política** preparada la política y aprobada por los diversos elementos representativos de la universidad, establecer un esquema que permita dar a conocer la política que se desea implementar
IV. **Definición de Roles** la política establecerá una serie de roles que jugaran los diversos elementos que configuran la comunidad universitaria, se trata de definir sus responsabilidades y entrenarlos para el cumplimientos de las mismas
V. **Requerimientos de Software y Hardware** una política requiere tener elementos que puedan detectar de manera proactiva posibles desviaciones y de manera punitiva si se comete una falta grave. Para poder cumplir con ello es necesario definir las herramientas existentes y como poder sacar el mejor provecho de ellas para el cumplimiento de las políticas que se van a implantar, y los requerimientos a futuro que optimicen la función que es esta estableciendo.
VI. **Plan de Implantación** la política requiere de un proyecto en el tiempo, en el cual se vayan cumpliendo por fases la implantación de criterios de seguridad, basado en Análisis de Riesgo.
VII. **Actualización** establecer las normas que permitan la actualización del esquema propuesto en el tiempo

A Manera de Prefacio a objeto de facilitar la lectura del presente documento, debo indicar que el mismo se encuentra dividido en Capítulos y Anexos, a excepción del capítulo 1, en el cual hago una introducción somera al problema de Seguridad de la información, el resto de los capítulos contienen anexos que complementan el marco teórico sobre el cual se sustenta el presente trabajo, por esa razón recomiendo ir al capítulo si busca información referencial y complementar con el anexo si se buscan aspectos más específicos.
De igual manera informo a los lectores, que esté trabajo se encuentra digitalizado en la página web: www.geocities.com/inspb001/seguridad_computacional. Igualmente si quiere comunicarse conmigo o requiere información adicional

respecto a este documento, debe hacer lo a través del correo electrónico inspb001@cantv.net o por el correo pbf11@hotmail.com, cualquier comunicación será respondida a la brevedad posible.

Pedro Brao F.
Caracas Abril, 2002

Dedicatoria: A Gilda, los muchachos y a mis alumnos de Seguridad en la Universidad Católica

Tabla de Contenidos

Anexo 6
Acceso al Medio

Anexo 7
Redes

Anexo 8
Virus

Capitulo I

Introducción

1. La inmutable naturaleza del ataque al igual que en cualquier sociedad, en la de la informática existen personas que interactúan y forman complejas relaciones sociales. El ciberespacio es un símil del resto de las interacciones del ser humano: existen comunidades que pueden ser grandes o pequeñas, comercio en el que hay acuerdos y desacuerdos, existen tretas digitales que son una copia de las existentes fuera del ciberespacio. Luego es perfectamente lógico estimar que conociendo el pasado podamos predecir el futuro, los ataques podrán parecer diferentes pero en su naturaleza serán iguales; el ratero manipulará las conexiones digitales y las bases de datos pero no utilizará para ellos ganzúas ni cizallas, el terrorista apuntará a los sistemas en vez de a los aviones pero la motivación y la sicología detrás de los ataques, es la misma.

En nuestro mundo la gran masa de dinero no esta en los bancos, sé esta moviendo a través de las redes, cada día se transfieren miles de millones de dólares y para ello tan sólo modificamos números en una base de datos. Mientras que el promedio de un robo a un banco por la vía armada apenas alcanza un promedio de 50.000 $[1], el ciberespacio se torna cada día más apetecible ya que el comercio y las transferencias a través de este medio se incrementan. Estimamos que las leyes no protegen al usuario ya que la data no pertenece a la persona que la suministra, pertenece a la organización que la colecta. Su información financiera pertenece al banco y la información médica a la clínica. Actualmente se instalan toda una serie de medidores electrónicos que suministran gran cantidad de información a las instituciones de servicio, pero también suministran gran cantidad de información a una organización delictiva que lo desee y por tanto a través de este medio obtenemos toda una serie de conocimientos acerca del comportamiento del ser humano aun en la intimidad del hogar ya que a través de los esquemas de control y comunicación, se puede seguir minuto a minuto la actividad de un recinto. En resumen podemos afirmar que siempre que el ser humano pueda de alguna manera explotar el valor de la información esta será explotada y utilizada en su provecho.

1.1. Cambio en la naturaleza del ataque las tretas que se utilizan son las mismas, pero el ciberespacio lo cambia todo, aunque el ataque persiga el mismo objetivo las técnicas del ataque al final son diferentes. Son más comunes y extendidas en la medida que la gente comprende su naturaleza, es muy difícil seguir su pista, capturar y detener a los infractores y la naturaleza del delito puede incrementarse en su magnitud. Internet tiene tres características que convierten lo anteriormente mencionado en realidad, cualquiera de ellas sola es devastadora pero las tres en conjunto son terroríficas: **La automatización, las acciones a distancia y la propagación.**

- ✓ **Automatización** se convierte en el gran aliado del atacante, analicemos el siguiente ejemplo como una prueba de lo mencionado, suponga un falsificador de monedas y que utiliza las mismas para hacer llamadas telefónicas, una vez que comienza el proceso, probablemente durante los primeros meses la compañía telefónica no tome ningún tipo de medida puesto que la magnitud de la acción no los esta perjudicando. Después de un largo tiempo utilizando estas monedas falsas, alguien en la institución telefónica se molestará y tratará de capturar al infractor, pero si se analiza la realidad observaremos que los accionistas de la institución no sienten ningún efecto como causa de este pretendido robo y por tanto muy pocos recursos se utilizaran para descubrir la treta. En el Ciberespacio, la situación es realmente diferente, ya que el computador se encarga de hacer la aburrida tarea de hacer una llamada, en contraposición con la situación anterior el estafador cibernauta pudiera estar durmiendo, y a la vez estar produciendo millones de llamadas, en una modalidad conocida como la técnica del "Salami" que le permitirá robar millones en pequeñas cantidades. En el mundo normal la ganancia producida por estas técnicas es marginal, pero en el ciberespacio es una fuente de altas ganancias.. El ciberespacio a su vez abre nuevos aspectos para explotar elementos como la privacidad que puede ser muy útil para una campaña de negocios. Las tarjetas de crédito y los datos de los compradores son de gran valor para el comercio, conocer donde se compra, hábitos de los compradores, que restaurantes frecuentan, que

[1] CSI, conferencia de Otoño noviembre 2001

tipos de vacaciones toman. La obtención de toda esta información es relativamente fácil ya que casi todo el mundo tiene nuestra información (bancos, hoteles, aerolíneas, comercios, clínicas, restaurantes, etc.). En la actualidad hay direcciones Web que coleccionan y venden este tipo de información, si combinamos estas bases de datos la cantidad de información que podremos obtener es inmensa.

- ✓ **Acciones a Distancia** tal como lo expresan los conocedores, Internet no tienen fronteras ni límites. Dos puntos no siempre están adyacentes, esto significa que un atacante no requiere estar cerca del sitio para cometer el delito, tiene la opción Internet en donde cada computador es equidistante del otro por tanto debemos prever la posibilidad de recibir ataques de cualquier parte del mundo y este fenómeno global complica las investigaciones y persecución del perpetrador. Dado que las leyes limitan a un país, pueden darse situaciones, de ser acusado por un delito en un país en donde la persona nunca ha puesto un pie. Esta diferencia de leyes entre estados y países pudiera llevarnos a una forma jurídica de alta tecnología, que algunas veces puede trabajar a favor del perseguidor, pero en otros casos puede actuar a favor del criminal. Cualquier grupo delictivo, bien organizado y con recursos puede preparar un ataque en gran escala en contra de una organización financiera y para ello buscaría un país cuyas leyes en el ámbito tecnológico no estén muy avanzadas, con policías fácilmente sobornables y sin tratados de extradición.
- ✓ **Propagación** la tercera diferencia es la facilidad con la que las técnicas exitosas se propagan por el ciberespacio. Si alguien logra decodificar la imagen de HBO, si su estudio no lo publica, el efecto sobre la institución será mínimo, pero si la información es transmitida, la historia es otra, HBO no tiene forma de detener esta propagación lo le que traerá serios problemas financieros, lo que convierte a Internet en una excelente forma de propagación y ataque, sólo el primer ataque en este medio requiere habilidades especiales. Todo el mundo podrá usar la información posteriormente y una vez liberada, será muy difícil evitar su propagación. Tal vez el ejemplo mejor de lo que supone la propagación son los virus, a raíz del sostenido crecimiento de Internet y los correos electrónicos. De acuerdo a un estudio presentado por la revista Computerworld[2], basándose en investigaciones llevadas a cabo por Computer Economics INC, las perdidas en el ámbito mundial motivadas por ataques de virus alcanzan para el año 1999 la cantidad de 12 billones de $, CBS News[3], estima que en el año 2001 se gastaron 12.3 billones de $, para limpiar los sistemas informáticos atacados por virus, este incremento se continuará experimentando en el 2002, de acuerdo con lo expresado por esta fuente informativa, que pronostica que el ataque por virus incluirá además otros tipos de equipos tales como los equipos móviles y teléfonos inteligentes

1.2. Tretas Digitales los ataques a los sistemas son fáciles de entender "Se puede obtener el máximo de retorno financiero atacando a un sistema, con un mínimo de inversión y riesgo "

1.2.1. Fraude los fraudes se han cometido contra todos los sistemas. Los comerciantes inescrupulosos han usado escalas rígidas para obtener beneficios de una manera fraudulenta. Mientras no se inventó algo que lo evitara las personas raspaban las monedas para obtener de ellas plata y oro, casi todos los objetos de valor han sido falsificados y a través de estas falsificaciones se obtienen millones de dólares. El comercio electrónico no tiene nada de diferente, tampoco las técnicas que usan los delicuentes. De acuerdo con el National Consumer League[4] los cinco delitos más comunes son: las ventas por Internet, ventas de mercancía en general, las subastas y las pirámides. La gente lee cierta información recibida por E-Mail y le parece atractiva, o visita una simpática página Web y envía una cantidad de dinero que le es solicitado a alguna oficina o un PO box y por alguna razón que desconocen, no reciben nada de retorno, pero si consiguen algo no se corresponde con lo ofrecido, su valor es mucho menor que el que se pagó. Tal como sucede en el mundo físico cientos de personas son estafadas en el mundo electrónico.

---

[2] 17/01/2001 por Brian Fonseca

[3] Diciembre 2001, Mils Abreu

[4] Julio 2001, Spohn

1.2.2. Ataques destructivos son trabajos llevados a cabo por terroristas, empleados que buscan acciones de revanchismo o Hackers que actúan desde lejos. En este tipo de ataques el infractor se pregunta "Cómo puedo causar el máximo daño atacando un sistema". Un ataque sigiloso permite silenciar un ISP por semanas. Un Hacker con una combinación de conocimientos e inmoralidad pudiera terminar con Internet. Tal vez uno de los mejores ejemplos con los que contamos de éxito en ese tipo de ataque lo realizó USA contra el sistema de Comunicaciones Iraquíes en el Golfo Pérsico, durante la guerra que ambos países sostuvieron.

1.2.3. Robo de Propiedad Intelectual la propiedad intelectual es más que secretos de negocios y sus bases de datos. Es también la versión electrónica de libros y revistas, la digitalización de videos, música y todo tipo de imágenes. La dificultad en este tipo de delito es como mantener el control y recibir la compensación apropiada por ser propietario de la información que se ha hecho pública. En 1977 Business Software Alliance, tuvo un contador en su página Web que contabilizaba las pérdidas de la industria debido a la piratería en 428$ por segundo es decir 1,5 MM $ por año. En la actualidad el 95% del software que se utiliza en la República China es pirata, mientras que en Canadá esta cifra alcanza al 50%[5] .

1.2.4. Robo de Identidad es de gran provecho conseguir un puñado de tarjetas de crédito a nombre de cualquier persona, conseguir dinero a través de ellas y luego desaparecer. Esto es lo que se conoce como un robo de identidad y esta experimentando un gran crecimiento como un modo electrónico de delito. Pero el caso tiende a complicarse ya que cuanto más elementos de identificación electrónicos aparecen se hace más sensible el robo de identidad, al mismo tiempo cuanto más sistemas electrónicos de reconocimiento de identidad aparecen, se hace más sencillo el robo de identidad obteniendo más provecho y con menos riesgos para los usurpadores. Además debemos tomar en cuenta que las personas se han vuelto muy descuidadas y dan información sensitiva a cualquier persona o institución que se la solicita. Es muy común que demos nuestra identificación anexando el número de cédula en un cheque, y es que somos confiados en exceso.

1.2.5. Robo de Marcas la identidad virtual para los negocios es tan importante como la identidad individual. Toma mucho tiempo y dinero obtener una identidad corporativa, esta identidad es mucho más que logos y jingles. Es el producto de construir edificaciones, servicios de atención a los clientes, cosas que se tocan, personas que sé intercomunican. En resumen una marca es reputación. Como los usuarios, los sitios Web que visitamos, la institución con la que vale la pena establecer una relación, etc. Cientos de compañías venden PCs, cuantas son reales y cuantas desaparecen por la noche. El Ciberespacio tiene muchas oportunidades para el robo de marcas. Es muy fácil hacer un ruteo y de hecho muchas instituciones lo han hecho de manera que su Web site pueda robar información de los Web Sites de la competencia. Estas prácticas ocurren incluso en grandes corporaciones para ejemplo tenemos que cuando MCI puso a disposición el 1-800-COLLECT, y se convirtió en un sitio muy popular, AT&T instituyo un servicio 1-800-C0LLECT, pusieron un cero sustituyendo la letra "O".

1.2.6. Privacidad y Violaciones la violación a la privacidad no es necesariamente un delito, pero pudiera serlo. Muchas de las violaciones a la privacidad son legales. La persona no es propietaria de su información. Si solicita crédito a un grupo financiero, este lo investiga y Ud lo consiente, conoce sus hábitos, sus patrones de compra, su estado financiero, su salud y otros aspectos. Toda esta información puede ser posteriormente vendida a quien la requiera sin su conocimiento ni consentimiento.

Existen dos tipos de violaciones a la privacidad ellas son ataques dirigidos y recolección de datos, son fundamentalmente diferentes. En un ataque dirigido el atacante quiere conocer todo acerca de una persona o una empresa, en ese caso hablamos de una cacería, en el segundo de espionaje y si es gobierno Inteligencia Nacional. La seguridad computacional sólo protege la información mientras está en el computador. La recolección de datos es el otro tipo de violación de la privacidad y el ataque esta dirigido a establecer correlaciones entre diversas bases de datos.

1.2.7. Bases de datos. Históricamente la privacidad sólo se relacionaba con la vigilancia, pero en 1960 la sociedad alcanzó un momento crítico, los computadores, pronto empezaron a almacenar información que derivaron en bases de datos que se iniciaron de manera individual, hasta formar las relacionales, posteriormente sucede un segundo momento crítico: las redes, lo que permite que las bases de datos se

[5] Scret & Lies, Bruce Scheneier

compartan. Más y más datos se están colectando y guardando por dos razones: es muy barato y por que día a día las personas están dejando mas huellas de su comportamiento, muy fácilmente digitalizables. Mucha de esta información almacenada es guardada, cruzada y correlacionada, mucha de la misma es disponible en línea, dando como consecuencia que sin saberlo tenemos un completo dossier almacenado al alcance de cualquier interesado, puesto que mucha de esta información sé esta comercializando. Existen grandes bases de datos sobre crédito que no están suficientemente protegidas y que además sus propietarios las comercializan, esta base de datos es fácil de correlacionar con otras de salud, financiera, costumbres, etc.

1.2.8. Análisis de Tráfico es el estudio de patrones de comunicación, no del contenido del mensaje pero si de ciertas características que pueden tener. ¿Quién se comunica con quien?, ¿Cuan cortas o largas son las respuestas?, ¿Qué tipo de comunicación sucede después de que cierto mensaje se ha recibido? Todos estos aspectos tienen relación con el análisis de tráfico y sus respuestas revelan una gran cantidad de información. A manera de ejemplo podemos decir que si cada vez que "B" recibe un cierto mensaje de "A" y en respuesta "A" remite cierto mensaje, se nos está indicando una cadena de comando en la que "A" es jefe de "B" quien está recibiendo ordenes y a su vez las está desviando a sus subalternos, pero si de repente "A" comienza a enviar largos mensajes a "B" se nos está indicando que algo está cambiando.

1.2.9. Vigilancia Masiva en Medios Electrónicos. Este tipo de tecnología requiere básicamente de herramientas de diagnóstico y análisis de tráfico ya que los equipos de intercepción deben ser capaces de caracterizar rápidamente la información interceptada, conociendo quien la envía, quien la recibe y cual es el tópico de la comunicación, mucho de ello puede obtenerse utilizando una máquina de búsqueda inteligente.

1.2.10. Ataques Publicitarios el ataque publicitario es conceptualmente simple. ¿Cómo puedo hacer que atacando a unos sistemas, me haga famoso?. Esto no es difícil un ejemplo fue cuando se logró la ruptura del esquema de encriptación de Netscape, por dos alumnos de Berkley en 1995. Ellos no tomaron ventaja del descubrimiento, por el contrario, se comunicaron con el New York Times. Los ataques publicitarios pueden ser costosos ya que los usuarios pueden abandonar las bondades de un producto a favor de otro después de un ataque. En muchos casos los bancos buscan callar los problemas acontecidos a fin de evitar la publicidad que alarma al público.

1.2.11. Ataque para negar el servicio la idea tras esto es muy simple hacer que algo deje de operar, es muy efectivo por que las redes existen para permitir la comunicación, aun si se logra detener el ataque será un triunfo para el infractor. Este tipo de ataque no requiere mucha técnica para llevarlo a cabo, sólo se requiere de un saboteo que es mucho más fácil que buscar las debilidades del software. Es el tipo de ataque más difícil de evitar.

Capitulo II

Políticas de Seguridad

2 Políticas de Seguridad de Información

2.1. Seguridad Computacional de manera general la seguridad computacional incluye entre otros rubros: control de acceso, gerencia de las cuentas y privilegios de los usuarios, protección de copias, protección de virus, medición de software, seguridad en bases de datos, la seguridad de la información que viaja a través de las redes.

Podemos definir Seguridad computacional como la prevención y detección de acciones no autorizadas, llevadas a cabo por los usuarios de un sistema computarizado así como la recuperación en caso de colapso.

2.1.1. Definiciones históricamente la seguridad de computación esta relacionada con tres elementos: **Confidencialidad, Integridad y Disponibilidad**.

- ✓ **La Confidencialidad** no es mucho más que la privacidad. El rol de la Seguridad Computacional es detener al usuario no autorizado a fin de que no pueda acceder a la información clasificada como sensitiva.
- ✓ **La Integridad** es difícil de definir de una manera precisa, podemos decir "cada pieza de información que tiene autorización para ser modificada lo será". La integridad asegura que la data no será alterada ni eliminada por alguien al que no le está permitido hacerlo.
- ✓ **La Disponibilidad** es el tercer pilar y ha sido definido a través de varios estándares de seguridad entre ellos cabe mencionar "La propiedad de ser accedido y usable al ser demandado por una entidad autorizada".Control de Acceso, confidencialidad, disponibilidad e integridad todos en conjunto se entremezclan para permitir actuar al control de acceso, queremos estar seguros que sólo el personal autorizado puede hacerlo

2.1.2. Modelos de Seguridad. Hay una gran cantidad de modelos utilizados para explicar la seguridad de Información, muchos de ellos fundamentados en el modelo del Departamento de Defensa de USA. En los 60s se utilizaban **Multilevel Security (MLS)** basados en la clasificación de la información y diseñados para manejar diversos niveles de clasificación de la información en un solo sistema. Posteriormente y derivados de los anteriores aparecieron otros modelo como el **Bell-La Padula,** que define sujetos, objetos y acceso a operaciones. Este esquema tiene dos reglas de seguridad la primera tiene que ver con la lectura de la data y la segunda sobre la escritura. Si un usuario tiene acceso a secretos, el puede acceder a la información clasificada hasta el nivel al que tiene derecho pero no puede acceder a información por encima de ese nivel (Top Secret. Si un usuario esta trabajando con información secreta, puede crear documentos que pueden ser accedidos por su propio nivel o un nivel superior, pero no puede ser accedido por un nivel inferior.) En resumen este esquema parte del principio de que un usuario no puede leer documentos con clasificación superior a los que tiene acceso y no podrá escribir documentos a un nivel inferior. Esto hace posible que se escriba un documento que no puede ser leído por la persona que lo escribió.

El modelo Bell-La Padula ha significado un gran avance pero tiene limitaciones. La principal es la concentración en la confidencialidad y la confidencialidad esta basada en el modelo militar. Otro elemento limitativo viene dado por el hecho de que a veces un individuo debe trabajar con data a la cual no tiene acceso. Si bien existen otros modelos como: **el Militar (MLS), Chinesse Wall y el de Clark-Wilson**, para los efectos de este trabajo, utilizaremos el modelo Bell-La-Padula, por ser a nuestro juicio el que mejor se aproxima al ambiente sobre el que hacemos este estudio.

2.1.3. Bases de Seguridad y Confianza muchos sistemas operativos incluyen esquemas de seguridad y esto tiene sentido ya que el mejor sitio para ubicar la seguridad es en las capas de más bajo nivel que es donde está ubicado el sistema operativo. Esto es una buena idea por diversas razones:

- Siempre es posible comprometer a un nivel, atacando al nivel inferior.
- Siempre es más fácil agregar seguridad en el núcleo del sistema.
- Siempre obtendremos mejor rendimiento al ubicar la seguridad a nivel de Sistema operativo

Al analizar los niveles de riesgo pasaremos elementos de seguridad en Linux y NT, sistemas que actualmente están muy en boga en el ambiente en el que realizamos el trabajo, el primero por ser un

sistema operativo de muy bajo o ningún costo, lo que lo ha popularizado entre el alumnado de la institución, el segundo es muy usado por los sistemas operativos de control de red que viene utilizando la institución.

2.2. Organizándonos para la Seguridad

En tecnología de información, varios factores están afectando de manera dramática la seguridad, así como la manera en que la misma sé esta implantando, ellas son la **Computación Distribuida**, en la cual los dueños de la información y los usuarios tienen sus propios computadores y redes que usan en la organización, la institución y en algunos casos al nivel de varias instituciones y países. Por otro lado el incremento continuo y la dependencia de los negocios de la Internet. **La naturaleza de la informática y su ubicación** las empresas, ponen la seguridad de la información en sus propios propietarios y en los usuarios de las mismas quienes ponen mayor énfasis en desarrollar de manera efectiva su trabajo que en proteger su información. La seguridad no es un requerimiento de muchas organizaciones, sin embargo de alguna manera están preocupados por resguardar su información y quisieran aplicar algún grado de seguridad a sus sistemas computarizados y a sus ambientes de redes.

Es el objetivo de acuerdo con lo expresado sugerir formas de asegurar la información en un ambiente de información distribuida y es necesario lograr de manera prudente conseguir niveles consistentes de seguridad en todos los ambientes.

2.2.1. Metodología general de seguridad para información distribuida la sugerencia general es manejar la información y su seguridad de manera indirecta a través de las gerencias de las organizaciones donde la información es requerida. Esta metodología por supuesto tiene que tener la aprobación de la alta gerencia y las autoridades a fin de forzar su cumplimiento a todo el personal. Para lograr esto debemos:

- ✓ **Conformar un comité** con representantes de todas las organizaciones a fin de que todas las áreas que procesan o manejan información se encuentren representadas, asegurarse que las resoluciones son conocidas por las autoridades, que las decisiones tomadas tienen su aprobación. Este grupo conformará la base que producirá posteriormente las políticas de seguridad de la empresa
- ✓ **Concienciar y Motivar**, informe a todos los niveles acerca de las tretas y vulnerabilidades, discuta casos específicos y permita que los usuarios propongan soluciones, supervise la actividad de los suplidores y contratistas a fin de detectar posibles negligencias, para cumplir con ese cometido se recomienda incluir estos criterios:
    - o Hacer de la seguridad parte del trabajo, exigir que la seguridad se incluya en los criterios de evaluación del personal, se requiere a través de su apreciación proporcionar recompensas y castigos.
    - o Mostrar la necesidad de ser cuidadoso, de evitar negligencias para ello utilizar métodos probados, asegurarse de que las organizaciones tratan seriamente las negligencias.
    - o Ilustrar a las organizaciones sobre las consecuencias de las fallas de seguridad usando para ello casos de estudio, enfatizar las pérdidas que han traído para las instituciones las actitudes negligentes.
    - o Demostrar la efectividad y lo fácil que es usar los sistemas de control y como pueden ayudarnos a reducir las pérdidas.

La gerencia debe inculcar en todos los miembros de la organización la seguridad como materia de interés organizacional, esto es lo único que garantiza que la seguridad se cumpla, sin requerir la presencia del personal de control.

Apuntemos al nombramiento de Coordinadores de Seguridad para todas las regiones y los departamentos de la institución, con ello pretendemos cubrir todo el ámbito empresarial, será función de estas coordinaciones las siguientes:

- ✓ Administrar la seguridad de los sistemas y sus accesos a través de la red.
- ✓ Identificar y autenticar a los usuarios, mediante la asignación de procedimientos de acceso (Signon y Password).
- ✓ Iniciar una fase de monitoreo físico de las oficinas que lleven como objetivo evitar que la información pueda ser difundida.
- ✓ Revisar los logs y reportar situaciones no usuales a la gerencia.

- ✓ Someter revisiones de los esquemas de seguridad por excepción.
- ✓ Proporcionar guías de seguridad.
- ✓ Hacer arreglos para el entrenamiento del personal.
- ✓ Identificar a través de las políticas de seguridad, los diferentes roles y sus funciones: Dueños, Proveedores de servicio, Custodios, Usuarios. Identificar en dichas políticas la responsabilidad de cada uno de ellos.

Estos coordinadores están ubicados en un área de gran responsabilidad y no deben ser los mismos que proveen el servicio de Computación Distribuida. Debe existir una organización de alto nivel responsable en la institución de la Seguridad de la Información, ellos son los encargados de establecer los estándares de seguridad y los controles que se requieren en situaciones de organizaciones y usuarios especiales. Esta organización debe publicar las políticas de seguridad, establecer de acuerdo con la plataforma de computación que se utiliza los estándares de seguridad recomendada, debe proveer un servicio de help desk, consultaría y entrenamiento en el área de seguridad. Las instrucciones y políticas deben ser publicadas en un lenguaje simple y de fácil comprensión para los usuarios. Esta unidad de igual manera debe conocer los nuevos servicios que se agregaran y recomendar la seguridad más conveniente para proteger la información que se correrá sobre dicha plataforma, debe igualmente investigar y conocer acerca de nuevos productos y técnicas de seguridad que están saliendo al mercado. Deben asegurarse que no hay excepciones en seguridad y si se requiere alguna excepción sólo es aplicable si es en beneficio de los objetivos del negocio. Proporcionar procedimientos a seguir en caso de excepciones, asegurarse que al utilizarlos la gerencia de la institución y la unidad de seguridad conocerán las razones de las mismas.

Se requiere obtener un inventario preciso a fin de determinar que se va ha proteger y mediante este conocimiento poder distribuir los recursos asignados para la protección de la información en las diversas plataformas. Dentro del inventario se requiere conocer que medidas de seguridad están vigentes. Quienes y por que tienen acceso a la seguridad crítica de la empresa.

Hacer seguimiento y revisar las desviaciones encontradas utilizando para ello las unidades de auditoria. El grupo de auditoria debe conformar una unidad que reporte con frecuencia fallas tanto a la gerencia respectiva como a la unidad de seguridad. Debe mantener la unidad de seguridad de manera muy clara su rol que no es el de vigilancia, es una unida técnica y de respaldo para la empresa. Los castigos que se deriven por el incumplimiento de las políticas deben ser manejadas por los Gerentes de las organizaciones usuarias.

2.2.2. Importancia de la Política de Seguridad si bien en cualquier ambiente una política de seguridad es importante, en un medio distribuido se hace más complicado puesto que constituye un reto el forzar a todos los usuarios de las áreas diversas de la institución a cumplir con los requerimientos de seguridad que se han establecido. Estas políticas de seguridad deben ser lo suficientemente claras y comprensibles, a fin de reducir las explicaciones e instrucciones que deban darse a las diversas organizaciones para saber que han comprendido el alcance de las políticas que se han establecido.

Las políticas deben incluir una descripción general, e identificación de las unidades que intervienen en el proceso y sus funciones, no debe utilizarse el nombre de las personas que ocupan los cargos y siempre debemos referirnos a los cargos propiamente dicho.

Si bien debemos ser lo más explicativos posibles, debemos en algunos casos generalizar a fin de que los cambios que se produzcan en un futuro no afecten el contexto de la política, por ejemplo una política que establezca "Cada usuario debe autenticarse por un método aceptable para la empresa" es preferible a usar el término específico "Cada usuario debe autenticarse por un password compuesto por seis caracteres"

La política de seguridad debe incluir en su texto de alguna manera los siguientes elementos:

- ✓ Importancia de los activos.
- ✓ Necesidad de seguridad.
- ✓ Leyes y regulaciones gubernamentales que apoyan la política.
- ✓ Roles del personal.
- ✓ Aplicabilidad al personal y los contratistas.
- ✓ Elementos, función y ámbito de la seguridad.
- ✓ Tipos, medios y formas que la política abarca.
- ✓ Información estratégica y táctica.
- ✓ Definición de pérdida.

- ✓ Clasificación de la información.
- ✓ Privacidad y su importancia.
- ✓ Identificación, recompensas y penalidades.
- ✓ Como reportar actitudes sospechosas y atentados contra la seguridad.
- ✓ Respuestas ante emergencias, recuperación, y Continuidad operativa.
- ✓ Información sobre el grupo de seguridad.
- ✓ Desviaciones y excepciones.
- ✓ Mantenimiento del manual.

Es imprescindible que todo el personal comprenda el ámbito que cubren las políticas que se están estableciendo, el documento debe tener plena aceptación y debe ser firmado por todo el personal como adherencia a las políticas que se han establecido, al personal nuevo que se integra a la empresa, se le debe instruir acerca de la seguridad de la información al momento de integrarse, lo anteriormente especificado, aplica igualmente para el personal contratista.

2.2.3. Bases de las políticas de seguridad debe estar enfocada al individuo, ser fácil de identificar, clara y cubrir todos los puntos a fin de que pueda ser aceptada por todos. Todos los usuarios deben conocer el porque de cada uno de los puntos. Las políticas de seguridad además deben:

- ✓ Ser consistente con el resto de las políticas corporativas.
- ✓ Aceptada tanto por las diversas gerencias de la institución como por la gerencia de red.
- ✓ Su aplicación se forzará utilizando los equipos software y hardware que posee la empresa.
- ✓ No debe estar por encima de las leyes de la nación, estado o municipio.

2.2.4 .Que hacer para tener una buena política de seguridad

- ✓ Debe ser accesible a todos los usuarios.
- ✓ Definir las metas de seguridad perseguidas.
- ✓ Definir de manera precisa cada punto.
- ✓ Mostrar claramente las responsabilidades de la organización.
- ✓ Definir la justificación.
- ✓ Aclarar los roles y responsabilidades.
- ✓ Determinar las consecuencias de su no cumplimiento.
- ✓ Definir el nivel de privacidad.

2.2.5. Políticas y Cronogramas en el **anexo 1**, podremos observar el esquema de política establecido y el cronograma propuesto para su completación, nuestro criterio es: que previo a cualquier esquema que suponga la implantación de políticas las autoridades deben comprender que si bien estamos buscando una solución técnica, el problema es netamente gerencial, y depende fundamentalmente de las autoridades la implantación, involucramiento y soporte de la solución propuesta

Capítulo III

3Análisis de Riesgo

3.1 Definición es el proceso de identificación de los activos que deseamos proteger y las tretas potenciales en contra de ellos. Un Análisis de Riesgos responde a las siguientes preguntas:

- ✓ Qué activos requiero proteger.
- ✓ Cuales son las potenciales fuentes de ataque contra mis activos.
- ✓ Quién desea comprometer mi red, que gana con ello.
- ✓ Cual es la probabilidad de que tenga éxito un ataque contra mis activos.
- ✓ Cuál es el costo inmediato si un activo es comprometido.
- ✓ Cuál es el costo de recuperación de un ataque.
- ✓ Cómo pueden los activos ser protegidos de una manera efectiva.
- ✓ Existe en la institución un grupo regulador que determine los niveles de seguridad requeridos.

3.1.2. Activos a Proteger suelen caer en alguno de los siguientes items:

- ✓ **Recursos Físicos** son recursos con forma física definida, incluye entre otras las estaciones de trabajo, servidores, terminales, Hubs, resto de periféricos, y todo equipo de computación.
- ✓ **Recursos Intelectuales** supone cualquier forma de información que juega algún papel en la organización y administración de la empresa. Incluye el software, información financiera, bases de datos, esquemas, planos, etc.
- ✓ **Recursos de Tiempo** es un importante recurso el tiempo, que en muchos casos no es tomado en cuenta al llevar a cabo un Análisis de Riesgo. Si evaluamos el costo que el tiempo perdido tiene para una organización, estamos seguros que este recurso no será dejado de lado.

3.1.3. Potenciales Fuentes de Ataque puede ser cualquier fuente que tenga acceso a la red, entre ellos podemos mencionar los siguientes elementos:

- ✓ Sistemas Internos.
- ✓ Acceso por las oficinas.
- ✓ Acceso por la WAN o un asociado.
- ✓ Acceso por Internet.
- ✓ Acceso a través de Módem.

3.1.4 ¿Quien desea comprometer mi Institución? tal vez es la primera pregunta que debemos hacernos al momento de iniciar un proceso de análisis de riesgo ya que es básico identificar las potenciales tretas y conocer de donde o de quienes pueden provenir estos ataques, a tal efecto debemos revisar:

1. Empleados.
2. Personal temporal, consultores.
3. Competidores.
4. Individuos con objetivos o puntos de vista radicalmente opuestos a su organización.
5. Individuos con deseo de venganza contra la organización o el personal.
6. Individuos que desean ganar notoriedad.

Todos estos elementos pueden variar dependiendo de la institución, pero lo importante y que debe ser tomado en cuenta es determinar **que tretas pueden utilizarse para tener éxito en un ataque y cuanto costará al atacante lograrlo.**

3.1.5. Cual es la probabilidad de ataque? una vez identificados los recursos, las fuentes de ataque y conociendo los que pudieran comprometer la institución, se hace necesario analizar estos puntos y determinar si tiene algún valor para el atacante la acción que quiere tomar, debe igualmente comenzar a realizar la apreciación de costo de este ataque a tal efecto procederemos con los siguientes pasos:

- ✓ **Cual es el costo inmediato para cada activo** listado determine el costo que implica un problema con el activo o su destrucción. Tenga en cuenta que el costo no es el principal problema al hacer esté análisis debe analizar implicaciones con el personal, las legales, las de imagen, etc.
- ✓ **Cual es el costo de recuperación** identificado el costo inmediato, se debe calcular el impacto financiero que tiene sobre la institución el proceso de recuperación. El elemento general que debe

guiarnos al tomar decisiones de protección, será que el costo que el elemento que deseo proteger debe ser mayor que el costo de su recuperación.

3.2 Análisis de Riesgo pocas palabras forman parte tan integral de la vida, del desenvolvimiento y desarrollo del ser y sobre la cual reposa, según se enfoque o manipule, el éxito o fracaso del hombre. Entre esas pocas, encontramos la palabra RIESGO. Vivimos en un mundo lleno de incertidumbres en el que constante y continuamente debemos analizar y escoger alternativas, tomar decisiones, asumir riesgos, lo que crea dudas y aprehensión sobre si estamos tomando la decisión correcta o no, si el riesgo es muy alto o no, si vale la pena tomarlo o no.

Cualquier acción o decisión que tomemos, pasiva o activa, va a representar un riesgo. Si nuestra acción es Pasiva, es decir cuando no tomamos una posición ni en Pro ni en Contra de algo, existe la incertidumbre de qué hubiese sucedido o cual hubiese sido el resultado si lo hubiésemos hecho o no y por lo tanto el RIESGO de haber dejado pasar una oportunidad. Si la acción es Activa, es decir, tomamos una posición determinada corremos el RIESGO de ganar o perder.

La vida intrínsicamente esta llena de peligros reales o percibidos. Si cruzamos una calle, hacemos inversiones, decidimos que vamos a comer o como nos desplazaremos de un sitio a otro, o escogemos una profesión..... De una manera u otra constantemente estamos tomando decisiones basándonos en riesgos y beneficios que una particular actividad nos proporciona o que sucedería si la rechazamos.

3.2.1 Definición Análisis de Riesgo, como un **cuerpo de conocimientos (metodología) que evalúa y deriva una función probabilística que un agente, efecto adverso, proceso industrial, tecnológico, industrial,..., pudiera ocasionar**

Existen muchas otras definiciones, entre ellas podemos mencionar:

- "Riesgo es la falta de certeza sobre el acontecimiento de una pérdida"
- "Riesgo es la posibilidad de que una institución o individuo sufra una pérdida"
- "Riesgo es un conjunto de circunstancias que representan una posibilidad de pérdida"
- "Riesgo es la incertidumbre de que ocurra una pérdida económica"

Si analizamos las definiciones anteriores podemos observar que a pesar de ser diferentes autores, las mismas coinciden en expresar que **riesgo es la incertidumbre asociada con algo que puede producir una pérdida.**

Se requieren una serie de elementos comunes para cualificar un proceso de Análisis de Riesgo, estos elementos son:

- ✓ Identificación del agente de riesgo.
- ✓ Relación-dosis respuesta (cantidad, intensidad o concentración de un agente para causar el riesgo).
- ✓ Análisis de exposición (qué se expone, quien, cuanto, como).
- ✓ Caracterización del riesgo (revisión de los elementos previos que han ocurrido y realización de cálculos basados en datos, con un soporte claro de todas las asunciones. Frecuentemente la conclusión es que se requiere más data o mejorar en la metodología ya que de la información disponible no se puede derivar una función probabilística que exprese de manera precisa la magnitud del riesgo).

Por el hecho de que el análisis de riesgo es una disciplina en la cual intervienen muchas disciplinas y de gran complejidad, se requiere de una apropiada cantidad de tiempo para enfrentarse con problemas de alta o media complejidad, tales como observar el tráfico al cruzar una calle o manejar un vehículo, Pero en procesos más complejos como cuando nos exponemos a sustancias tóxicas, radiación o la probabilidad de un desastre en una planta nuclear, el análisis de riesgo formal se hace necesario a fin de producir recomendaciones razonables (en algunos casos óptimas) para determinar de manera precisa el riesgo al que nos exponemos.

El Análisis de Riesgos tiene su base en la teoría de la probabilidad y el desarrollo de métodos científicos que permiten establecer relaciones causa-efecto. Blas Pascal introduce la Teoría de la Probabilidad en 1657. En 1693 Edmond Halley prepara las primeras tablas de esperanza de vida y en 1792 La Place desarrolla el primer prototipo de un análisis de riesgo cuantitativo al calcular la probabilidad de muerte si se utilizaba o no la vacuna contra la viruela.

3.2.2 Soluciones Cualitativas y Cuantitativas fundamentalmente existen dos esquemas diferentes que pueden ser utilizados para el establecimiento de riesgos ellos son los **Cualitativos y los Cuantitativos**.
Los primeros esfuerzos para el desarrollo de una metodología para llevar a cabo un proceso de Análisis de Riesgo fueron llevado a cabo por el **National Bureau of Standards**, conocido en la actualidad como National Institute of Standard and Technology (NIST), quien en 1974 produjo el documento **FIPSPUB-31**, Seguridad Física y Gerencia de Riesgos para el Procesamiento Automático de Datos. En 1979 se produce una actualización **FIPSPUB-65**, "Guidelines for Automated Data Proccesing Risk assessment". Los esfuerzos para manejar un esfuerzo cualitativo desde un principio fueron complicados, primero por que no se han mantenido métricas independientes y confiables que nos den medidas de los riesgos, segundo aunque el proceso luce simple en su conceptualización es bastante complejo en su ejecución, tercero se obtiene una gran cantidad de información que requiere un proceso complejo de mapeo, pareo y cálculo que finalmente nos permita presentar un modelo de riesgo. Todo ello lleva a la presentación de una actualización OMBA-71, que nos presentaba una metodología para manejar resultados cualitativos, creando tablas que asocian riesgos y su valor con estimaciones de su impacto. Todas las publicaciones e información referente a estos estándares pueden conseguirse en la página Web de NIST, cuya dirección es www.nist.gov/publications
Tal como se muestra en la gráfica, se ha tratado de determinar de una manera subjetiva el valor de la disponibilidad de diferente información y su disponibilidad en opinión de diversos personeros de la empresa, lograda a través de cuestionarios y entrevistas.
3.2.3 Procesos de la Gerencia de Riesgo para que el Gerente de riesgos pueda cumplir con todas sus responsabilidades, debe seguir una metodología cuyos pasos en forma general son:

- ✓ Identificar y analizar todas y cada una de las exposiciones a pérdida.
- ✓ Medir y evaluar las exposiciones a pérdida ya identificadas y analizadas, supone la estimación de la frecuencia de las pérdidas, la magnitud o severidad de las mismas y su efecto económico.
- ✓ Como manejar los riesgos, buscar alternativas, supone buscar la mejor y más económica de las alternativas para manejar los riesgos, ya sea por eliminación, prevención, reducción, transferencia, retención o alguna combinación de ellas.
- ✓ Implementar, controlar y manejar el programa de Gerencia de Riesgos, incluyendo la evaluación constante del mismo para verificar su eficacia y aplicabilidad o su adaptación según las circunstancias existentes.

3.4 Un caso práctico para la mejor comprensión del proceso de riesgo para un centro de computación he querido presentar un caso práctico que clarifique la gran cantidad de conceptos que hemos utilizado y determinar cuando y como usarlos.

3.4.1. Revisión Preliminar Al comenzar a revisar una institución a objeto de determinar su exposición hay ciertas cosas históricas que debemos conocer de la institución tales como:

- ✓ Que software / hardware ha fallado en el pasado y cuales han sido las consecuencias.
- ✓ Existe un "Plan de Contingencia?", Esta el mismo actualizado?, si la respuesta a alguna de estas dos preguntas es negativa debemos preguntarnos la razón.
- ✓ Puede la institución operar fuera de línea, existe algún tipo de redundancia.
- ✓ Cual es la reducción de la eficiencia en ese caso

3.4.2. Fase de Diagnóstico con el conocimiento que nos da la fase preliminar que de alguna manera nos indica el riesgo general de la empresa, pasamos a la fase de diagnóstico, en ella nos enfocamos a los procesos de la institución y los riegos cualitativos y cuantitativos esta fase tiene diversos pasos, entre los cuales cabe mencionar:

- ✓ Identificación y Clasificación de Productos y Servicios implica el conocimiento del "a que nos dedicamos, saber exactamente que producimos"
- ✓ Identificación de los Productos Críticos para quien producimos y que valor tiene el producto que entregamos, que pasa si el producto se retarda o si no se puede ofrecer por alguna causa endógena o exógeno.
- ✓ Identificar y clasificar los riesgos supone una serie de trabajos con los usuarios a fin de poder determinar como afecta a cada gerencia o departamento el riesgo de que un producto o servicio no

llegue a su organización, determinar de igual manera el tipo de riesgo al que nos enfrentamos, si es interno podremos evidentemente ejercer acciones para reducirlo, pero si es de carácter externo tendremos que buscar la manera si es posible de reducirlo.

- ✓ Matriz de Riesgo una vez levantada la información anterior conjuntamente con el usuario, podremos obtener una matriz.

En el **anexo 2**, haremos un análisis pormenorizado, explicaremos algunos elementos de riesgo estudiados, ponderaremos el riesgo y estableceremos un plan que nos lleve a disminuir los riesgos encontrados

Capitulo IV

Business Continuity en Ambiente distribuido

4.1 Introducción Actualmente las organizaciones en su esfuerzo de reducción de costos están simplificando los niveles de gerencias mientras implementan matrices más complejas de control y reporte. Los sistemas distribuidos facilitan la factibilidad de estas reformas al mover el control de la información cerca de la fuente que la emana, el usuario final. Pero en este nuevo cuadro, la seguridad de la información incrementa su riesgo. Los ambientes tradicionales son fáciles de controlar, la información emana de su fuente centralizada, se desarrollan políticas, estándares y guías generales para la protección y seguridad de la base de información de las instituciones, además se difunde esta información a todos los usuarios y posteriormente se crea el mecanismo que fuerza el cumplimiento de las políticas establecidas. En los ambientes distribuidos, el personal de seguridad de información generalmente es requerido para que desarrolle planes de recuperación fuera del contexto tradicional, para ser de esta manera, parte de un esquema de recuperación completo del negocio. La recuperación de los sistemas de esta manera pasa a ser una parte del Business Recovery. **El éxito de un Business Continuity Plan (BCP)**, por tanto descansa en la capacidad que tenga la institución para integrar el esfuerzo de la recuperación de los sistemas dentro de un plan integral de recuperación de la empresa al momento de un desastre.

4.2 BCP... Los procesos de las distintas áreas de la institución deben ser tomadas en cuenta al momento de definir un BCP, el proceso en si mismo sigue los pasos de cualquier problema o del "Proceso científico", para ello desarrollamos una hipótesis y probamos la veracidad de la misma..... pero el proceso de BCP es iterativo y en la realidad, al momento de una contingencia es cuando podemos conocer si la hipótesis formulada funciona o no, por ello se vuelve imperativo que el plan se pruebe de manera continua y constante, todo esto, tomando en cuenta su importancia que no es otra sino la supervivencia de la institución. Las fases por las que debe pasar un proceso de Disaster Recovery Plan (DRP) son:

- **Concientización y Descubrimiento** comienzan en el momento en que un grupo de profesionales (Recovery Planning Team), identifica y determina los posibles y admisibles elementos que pudieran alterar la buena marcha del negocio, estos elementos son evaluados y se planifica el esfuerzo que supone llevar a cabo esta primera fase del proceso, los siguientes criterios deben ser tomados en cuenta en esta etapa:
    - A que se dedica la empresa (Core Business).
    - En que área del país esta ubicada, ¿tiene más de una ubicación?
    - Que medidas de seguridad se tiene implementadas.
    - El nivel de cumplimiento y concientización de las políticas, si es que están implementadas.
- **La adhesión de la alta gerencia a dichas políticas y procedimientos** una parte muy importante del proceso implica instruir a los empleados acerca de la exposición a la que se enfrenta la empresa y ellos mismos, que medidas deben ser tomadas para disminuir dicha exposición. En lo referente a sistemas de información que riesgos existen, que información es vital para la organización, que información es propiedad y que grado de confidencialidad tiene para el negocio, cuando una interrupción se considera catastrófica. Debe determinarse cuan extensa puede ser una exposición y el lapso de la recuperación, que operaciones son impactadas, las medidas de seguridad que deben ser tomadas, como minimizar las exposiciones.
- **Evaluación del riesgo** aspecto analizado ampliamente en el capítulo anterior.
- **Mitigación** básicamente cumple con dos objetivos: disminuir la exposición de la empresa y minimizar las posibles pérdidas
- **Preparación** delinea lo que debe hacerse adicionalmente, para que la mitigación pueda funcionar en caso de que alguno de los eventos previstos ocurra, todo basado en la percepción de lo que pudiera pasar y de quienes tomarían cual acción, de igual manera identifica los alternos (personal que reemplaza al responsable por ausencia total o parcial) en caso de que el personal clave previsto no pueda tomar la acción indicada, pregunta si el edificio sede puede ser ocupado en caso de no ser posible desde donde se operará, que se requiere para operar desde este sitio alterno, que soporte computacional se requiere en esta nueva locación, que esquema comunicacional se utilizará, que

distribuidores y suplidores de servicio deben ser contactados. Todas estas son algunas de las preguntas que debemos hacernos y responder en nuestros planes de contingencia.

- **Pruebas** determina la viabilidad de los planes establecidos y determina a su vez si existen omisiones, si se han hecho asunciones inválidas o postulado soluciones inadecuadas. Por otro lado las organizaciones no son estáticas por lo tanto los elementos de cambio imponen una frecuencia razonable de cambios.
- **Respuesta y Recuperación** en esta parte del plan se detallan de una manera individual los roles específicos de cada quien como parte de un grupo predeterminado que debe cumplir con roles específicos entre ellos: respuesta a la emergencia, determinación de los daños, deberes de los operadores en caso de emergencias y cualquier otro aspecto que la crisis que se ha presentado pudiera demandar.

4.3 Planificación Departamental un BCP debe ser visto básicamente como una recopilación de planes establecidos por los departamentos para continuar operando en caso de una contingencia, por tanto, cada departamento debe determinar cual son sus procesos y dentro de cada uno de los procesos cuales son sus prioridades. Con esta información la alta gerencia determina las prioridades.

- **El rol de tecnología de la información** el departamento de Informática no puede ser responsable de crear los planes departamentales de contingencia para el resto de la institución, pero si, debe tomar un rol de liderazgo en los planes que están desarrollando los diversos departamentos, ya que posee una mejor apreciación y comprensión del flujo de información en las diversas organizaciones
- **Dependencias Ínter departamentales** en muchos casos, al ser revisados los planes departamentales y sus consecuentes prioridades, se presentan conflictos motivado a que los departamentos al hacer sus planes identifican sus propias prioridades y no se ven como parte de la empresa, por lo tanto no toman en cuentas necesidades que para ellos son de poca monta, pero reviste gran importancia para otros departamentos. Informática, puede remediar estas discrepancias por su rol como líder y revisor de los planes departamentales.
- **Dependencias Externas** en las diversas fases que analizamos anteriormente, se pudo determinar los servicios externos que recibimos, en muchos casos los departamentos piensan que estos servicios están fuera de sus funciones básicas. Es una función básica dentro del plan el establecimiento de un procedimiento que permita continuar este servicio en la nueva locación seleccionada.

4.4 Operaciones Externas(outsourced) parte o la totalidad de las operaciones que venían llevando a cabo los departamentos se pasan a terceros, con la idea de que la empresa cumpla con las funciones neurales, las que mejor sabe hacer y que comprende su razón de ser. Deja las actividades complementarias a terceros, contratando para ello estas tareas. Desde el punto de vista de BCP, esto se convierte en un área clave, en esta parte el contratista debe convertirse en un aliado que contribuye a la continuidad del negocio. El responsable del plan debe velar por que el suplidor de servicio cumpla con su parte y que pruebe que su rol en caso de contingencia funciona perfectamente.

4.5 Exposiciones Internas y Externas los sistemas stand-alone adquiridos por algunos departamentos para propósitos especiales, frecuentemente, no están conectados a la red de la empresa y por ello no son tomados al momento de requerir prácticas específicas de seguridad.

4.6 Información al grupo Gerencial de los Riesgos. Es decisión enteramente gerencial la determinación de cuanto riesgo esta dispuesto a soportar, pero Informática debe alertar a la alta gerencia de las decisiones tomadas.

4.7 Políticas la mejor manera para comenzar la implantación de un sistema o una estrategia de resguardo, es definir y conseguir la aprobación de la alta gerencia de políticas y procedimientos de operación y estándares, requeridos para salvaguardar la institución en caso de desastre, estos elementos deben ser de obligatorio cumplimiento por todos los departamentos y su personal.

4.8 Capacidad de Recuperación basándonos en la información recogida por los diversos departamentos y conociendo las prioridades aprobadas al más alto nivel, Informática tiene que diseñar la configuración de un sistema intermedio, dimensionado al tamaño requerido, permitiendo a la empresa la continuidad operativa después del evento

4.9 Restauración de la Empresa es también una obligación de Informática, la planificación de los pasos que deben seguirse para volver la empresa a su situación anterior al desastre y la restauración completa de las operaciones.

4.10 Planificación para el ambiente distribuido determinada la magnitud de la recuperación que se desea llevar a cabo, el equipo debe tomar en cuenta los siguientes factores:

- **Protección de las redes LAN** dos son las razones fundamentales por las cuales se construyen los Centros de Computación, una tiene que ver con las condiciones ambientales inapropiadas donde se ubican los equipos en los departamentos. La segunda se refiere a las labores de control, en algunos departamentos inexistentes. Si bien esto se cumplía en los ambientes de los centros, en la actualidad podemos observar toda una variedad de equipos en ambientes inapropiados.
- **Gerencia Propietaria** conocer donde las organizaciones mantienen sus activos de computación (hardware, software e información) es crítico para los esfuerzos de recuperación. Informática debe estar vigilante de todas las estaciones de trabajo que utilizan las organizaciones, si están conectados a una red o no, su configuración específica, que software reside en ella, a que funciones soporta. Estos aspectos deben ser tomados en cuenta al momento de la toma de decisiones en caso de contingencia.

4.11 Integridad de la Data la información es uno de los aspectos que la institución debe preservar con mayor cuidado, misma no puede ser reemplazada en caso de pérdida o destrucción. Por tanto el usuario debe trabajar conjuntamente con el especialista de Informática, a fin de, poder asegurar que la información que la empresa posee es recuperable al momento que lo requiere. Desde políticas de respaldo, su frecuencia, donde deben guardarse los respaldos, la verificación de que los respaldos se están ejecutando de manera correcta, todo ello es lo primero que se debe verificar como elemento básico de mitigación. Ninguna estrategia de recuperación tendrá validez, si no puede recuperar y mantener la integridad de su información

4.12 Estrategia de recuperación de redes los planes de contingencia tienen como primer objetivo la supervivencia de la empresa. Esto supone tomar en cuenta ciertas previsiones, dada la limitada capacidad para soportar los sistemas que la empresa requiere para operar sus procesos prioritarios en las primeras horas posteriores al desastre. Para ello debe tomar en cuenta los siguientes aspectos.

- **Tolerancia de fallas contra redundancias** tolerancia de falla significa, que ningún punto debe fallar al cesar de funcionar el sistema principal, la redundancia y duplicación de los componentes claves es la base de la tolerancia contra fallas
- **Sitios alternos y Dimensionamiento del Sistema** una vez que las prioridades de una empresa se han determinado, es necesario, dimensionar la capacidad requerida para soportar aquellas prioridades que en las primeras horas se han decidido que deben estar operativas, a esto deben agregarse los requerimientos de los primeros días y posteriores semanas independientemente de la táctica que se siga con respecto al respaldo(Hot Site, Convenio con Tercero o Centro alterno de la propia institución), es muy importante hacer una buena apreciación en este sentido, pues el convenio que se ha establecido no permite cambiar la estimación inicial realizada
- **Respaldos adecuados y seguro almacenamiento Off-site** este proceso debe estar basado en políticas establecidas por la empresa que lleven a identificar la información vital y como debe ser manejada para conservar su integridad. La frecuencia de los respaldos vendrá indicada por el flujo de trabajo de la empresa y la volatilidad de la información, la recomendación general es: los servidores deben ser respaldados diariamente, los archivos claves al menos una vez a la semana, la misma frecuencia debe darse para las estaciones de trabajo que manejan información crítica para la empresa. De igual manera los planificadores de contingencias deben decidir cuando los respaldos deben ser llevados Off-site. La seguridad debe ser igualmente un punto importante y al trasladar la información al Off-site deben tomarse precauciones especiales puesto que la información más importante esta siendo trasladada y alguien pudiera tratar de atentar y apoderarse de la misma. A partir de 1988, han aparecido diversos productos que asisten al administrador LAN en la fase de respaldos, todos estos productos ofrecen encriptación, compresión de la información lo que lo hace muy efectivo para obtener respaldos remotos, por otro lado el concepto de Electronic Vaulting, que permite interconectar la empresa con su sitio de respaldo ha sido implementado con mucho éxito. En el **Anexo 3**, en la lámina "Recuperación y costos, mostramos de manera detallada las alternativas actuales existentes en el mercado.
- **Adecuada Administración LAN** hacer un seguimiento de cambios y mantener un inventario actualizado del software y hardware existente, es fundamental para el proceso de recuperación, para ello se recomienda un programa de auditoria que con cierta frecuencia recorra todos los elementos de la red y muestre los cambios que se han presentado, es de hacer notar que la política debe establecer

una estrecha relación entre los procesos de *Control de Cambio, Control de Problemas y Plan de Contingencia.*

- **Pruebas** el éxito de un esquema de recuperación, tiene relación con la extensión de las pruebas que se hayan realizado, las pruebas y el entrenamiento son reiterativos y necesarios, ello nos permite mantener los planes actualizados, y determinar la viabilidad de los procesos que suponen la recuperación al instante de un desastre.

4.13. Planes de Respaldo el plan de respaldo especifica el tipo de backup que mantendremos en nuestras instalaciones, entendiéndose por instalación tanto las internas como las externas y otras áreas que pudieran ser requeridas si el plan así lo considera. La frecuencia con la que las organizaciones se comprometen a llevarlo a cabo, los procedimientos que utilizarán, la ubicación de los recursos de respaldo, las locaciones en donde los recursos se recuperarán y en donde se reiniciarán las operaciones, el personal responsable de reunir o trasladar la información y reiniciar las operaciones, la prioridad que se asigna a los diversos sistemas y el lapso de tiempo en el cual se enmarca el proceso de recuperación.

4.13.1 El Backup por muy cuidadoso que seamos siempre estaremos expuestos a la pérdida de la información, y la única forma de recuperarnos ante ello es si tenemos un buen proceso de backup, sin él no puede funcionar ningún BCP. La totalidad o parte de la información se puede perder por destrucción o corrupción incidiendo en ello alguno de los siguientes tipos de fallas:

- **Error en la aplicación** un programa de aplicación puede actualizar la información de manera incorrecta por que tiene un bug. Usualmente en estos casos se produce un error localizado sólo en parte de la información ya que en la mayoría de los casos el error no cubre la totalidad de la misma
- **Error de Software** el sistema operativo, un programa utilitario o algún componente de software contiene un bug, que produce actualizaciones erróneas de la información, se corrompe la data, pudiendo ser el daño producido muy extenso.
- **Falla de Hardware** a pesar de la alta disponibilidad de muchos componentes de hardware, los problemas con los equipos continúan ocurriendo, estas fallas pudieran ser menores y pasajeras, como resultado de ello sólo ocurren problemas menores y fácilmente localizables, pero pudieran ocurrir problemas de mayor gravedad y permanentes, como podría ser la destrucción total de un disco.
- **Error Procedimental** un operador o usuario podría producir un error que podría dañar completamente la información. Por ejemplo que se produzca un error en el proceso de recuperación de un archivo, en cuyo caso el daño que se puede producir depende de la naturaleza del error que se produzca.
- **Falla Ambiental** Una falla ambiental, como una inundación, fuego o sabotaje, puede ocurrir en cualquier instante y extenderse por toda la institución. El almacenamiento de los backups fuera del área es imprescindible en estos casos. Es por ello que se requieren controles que permitan la recuperación de la información en el caso eventual de una pérdida, lo que nos lleva a buscar estrategias de recuperación y respaldo. Todas las estrategias implican tener una versión anterior y un log de transacciones o cambios a la información. Si un programa de actualización, crea una versión nueva de un archivo, la versión vieja y las transacciones son requeridas para la recuperación de la nueva versión. Pero si el respaldo se lleva a cabo in place, se requerirá un dump de la base de datos y un respaldo de las transacciones que la alteraron, desde el momento en que se llevo a cabo el dump a la base de datos.

4.13.2 Estrategias de Backup pueden tenerse dos esquemas en el primero la totalidad de la información debe ser restaurada, si la base de datos se ha perdido. Esto implica utilizar una versión anterior de la base de datos y un log de transacciones o cambios que han ocurrido desde el momento en que se ha realizado el Dump. En el segundo esquema una parte de la información debe ser recuperada por que presenta inconsistencias, el proceso supone reparar las actualizaciones que ocasionaron el daño, este debe ser un proceso preciso y seguro que nos permita llevar a cabo la restauración siguiendo el orden señalado en el procedimiento establecido. Cualquiera que sea la causa, las principales estrategias que aplican para el proceso de recuperación son las siguientes:

Abuelo, Padre, Hijo es una de las estrategias más conocida y antiguas que existen, evolucionó en la época en que las cintas magnéticas eran el medio predominante, pero aplica a cualquier medio de almacenamiento. Cuando la versión que se esta utilizando (**el hijo**) se pierde o presenta algún daño, la recuperación se lleva acabo utilizando la versión anterior (**el padre**) y el log de transacciones que lo

actualizará y reproducirá la versión del hijo dañada, pero si la versión del padre presenta también problemas, debemos recurrir a **el abuelo** y las transacciones que generaron al padre, para así poder proseguir el esquema de recuperación. Dos condiciones deben cumplirse para que esta estrategia funcione. Una es que los respaldos deben permanecer intactos esto es que los registros que han cambiado y los que no lo han hecho deben estar en el archivo y segundo es que el archivo de transacciones también debe permanecer intacto. Esto funciona perfectamente cuando los datos son almacenados en cinta, pero debemos evitar qué todo el almacenamiento se haga en sitio, ya que las transacciones re escriben la información, desapareciendo con ello parte de la información necesaria para la completa recuperación. La mayor ventaja de este proceso es su simplicidad, pero a su vez presenta algunas desventajas entre ellas cabe mencionar que no funciona muy bien cuando las transacciones concurrentes actualizan la base de datos, tampoco es muy eficiente cuando se daña parcialmente la base de datos y hay que reconstruirla desde una versión anterior. Otro problema que presenta es que la base de datos no puede ser accedida durante el proceso de recuperación.

Estrategia de Mirroring consiste en mantener dos copias completamente separadas de un archivo y actualizar ambas simultáneamente, para que idealmente funcione es conveniente que las dos copias no residan en la misma ubicación, esto trae como ventaja que nos protege contra fallas en el equipo y contra problemas ambientales que pudieran presentarse. En caso de que no pudieran estar físicamente separadas sólo nos protegería contra fallos del equipo. Para que esta estrategia funcione, debemos plantearnos dos interrogantes, la primera es el tiempo que podemos tener nuestra base de datos fuera de servicio, la segunda tiene que ver con las transacciones que se ejecuten durante ese periodo. Para solventar esto debemos tener en cuenta que el equipo quedará fuera por un periodo corto de tiempo mientras redireccionamos la base de datos, además es imprescindible mantener un log de las transacciones que ocurrieron durante el periodo que se presentó la falla y el que se detectó. Una vez redireccionada la base de datos debemos actualizarla con el log de transacciones para poder poner nuevamente la base de datos en funcionamiento. La ventaja que presenta esta estrategia es el corto tiempo requerido para reiniciar el proceso, esto es de gran importancia para empresas que procesan reservaciones en línea o para bancos, sistemas en los cuales la caída del equipo es intolerable, y el costo que implica no tenerlo funcionando supera con creces el costo de la redundancia propuesta. Pero igualmente tiene la desventaja del costo que supone un esquema dual al cual debe adicionar el costo de transmisión. Además de lo anterior, esta estrategia no protege contra daños provocados por la corrupción de la información ya que al mantener archivos en paralelo, al corromperse el primero, también lo hará el segundo.

El **Anexo 3**, ampliamos los conceptos de Respaldo, recuperación y administración del almacenamiento y mostramos ejemplos de implementación.

Capítulo V

Seguridad Física

5 Seguridad Física puede definirse como una serie de lineamientos procedímentales o físicos que se utilizan para defender un perímetro. La Seguridad Física incluye los siguientes renglones:

- **Control de Acceso**
  - Cerraduras y Llaves (Control de acceso).
  - Alarmas.
  - CCTV y Control Perimetral.
- **Control Ambiental**
  - Supresores de Filtros.
  - Reguladores de Voltaje.
  - UPS.
  - Control Incendios y otros.

El proceso de seguridad física comienza por entender las ocho distintas fases que intervienen en el proceso de seguridad y continua por entender las tretas y riesgos a los que se enfrenta la organización en la que se instalará el esquema de seguridad. Sólo después de haber comprendido lo anteriormente expuesto es que debemos comenzar a considerar los equipos y el sistema que utilizaremos para asegurar los activos que deseamos proteger. Las fases del proceso de seguridad son:

1. Anticipación.
2. Disuasión.
3. Prevención.
4. Detección.
5. Respuesta.
6. Aprensión.
7. Recuperación.
8. Castigo.

5.1 Control de Acceso: cualquier barrera de seguridad debe ser capaz de distinguir entre personas autorizadas, personas no autorizadas y visitantes. Esta discriminación puede ser ejercida por Guardias de Seguridad o por esquemas automáticos de Control de Acceso, esta basada en uno o más de los siguientes aspectos:

- **Identificación**.- *¿Quién es la persona?*
- **Password**.- *¿Qué conoce la persona*?
- **Llaves, tarjetas, etc**.- *¿Qué tiene la persona?*

5.1.1 Principios de Control de Acceso todo sistema de control de acceso se rige por los siguientes principios:

- La simple posesión de un elemento de Control de Acceso no garantiza privilegios para el acceso.
- Cuanto más sensible es el activo que se desea proteger más selectivos deben ser los mecanismos de control de acceso.
- Ninguna persona tendrá por su rango o posesión garantizada el acceso, custodia o conocimiento de la información sensitiva.
- Toda entrada debe ser supervisada.
- Debe existir un estricto control de visitantes en las áreas donde hay material o información sensible.

5.1.2 Elementos Portables de Control de Acceso un elemento portable de Control de acceso, el cual tiene registros de información pregrabados, que además el sistema de Control de acceso ha sido programado para

reconocerlo, permite a su poseedor acceder a un área determinada. Estos elementos al ser insertados en una lectora, si poseen el código requerido, garantizan el acceso a dicha área. En principio el concepto no se diferencia en nada del concepto de llave y cerradura que hemos venido utilizando por años.
Pero los modernos sistemas electrónicos de Control de Acceso, ofrecen una serie de ventajas frente a la vulnerabilidad de las llaves y las cerraduras y entre ellas cabe mencionar:

- Las llaves y cerraduras están limitadas a un número de combinaciones, en los sistemas industriales 10.000, los sistemas electrónicos pueden poseer millones de combinaciones posibles.
- Las llaves pueden ser duplicadas con relativa facilidad y a un bajo costo, los sistemas electrónicos requieren de alta tecnología para lograr su cometido.
- Mientras que la llave tiene como objetivo sólo dar acceso a una determinada área, los sistemas electrónicos pueden adicionar una compleja lógica que permite además de dar acceso proveer a la empresa de una serie de mecanismos de control.
- En su forma más simple el sistema electrónico de Control de Acceso utiliza un formato tipo tarjeta de crédito, alrededor del 75% de los sistemas ofertados, utilizan este formato, independientemente de la metodología utilizada (banda, proximidad, Wiegand, Inteligente).

5.1.3 Los códigos de los sistemas Portables Existen una gran variedad de tecnologías para almacenar la información requerida en una tarjeta de control de acceso, la misma depende de dos factores, el tamaño de la tarjeta, la cantidad de bits que pueda almacenar y la metodología que se utiliza para almacenar y acceder a la información. En el caso de una tarjeta magnética podremos decir que *un bit ocupa en promedio un espacio de 3mm* y las combinaciones que pueden llevarse a cabo alcanzan a:

- 1 bit proporciona 2 combinaciones
- 5 bits proporcionan 32
- 10 bits aproximadamente 1000 combinaciones (1024)
- 15 bits aproximadamente 32000 combinaciones
- 20 bits aproximadamente 1000000 de combinaciones
- 30 bits aproximadamente 1000000000 combinaciones

Tomando en cuenta que el espacio promedio de grabación en una tarjeta de banda magnética, es de 850 mm, podemos deducir que por tarjeta en teoría se pueden grabar sobre 250 caracteres, es por ello que los sistemas de control de acceso utilizan el espacio extra que les provee el tamaño de la tarjeta para almacenar información adicional y con ello se logra entre otras las siguientes ventajas adicionales

- Acceso por hora del día y por área
- Información para un sistema de log que permite conocer quién paso y a que hora por determinada área
- Sistemas de Control de personal (nómina)
- Cargos diversos por compras, etc.
- Para lograr este cometido, el Sistema de Control de Acceso debe ser controlado por un sistema centralizado y en cada tarjeta debe estar grabado un número de identificación. El sistema central utiliza una tabla que relaciona el número de tarjeta con la identificación del empleado y a través de este esquema, permite que se lleven a cabo las transacciones correspondientes.
- En caso de falla en el sistema central, establece un esquema de contingencia que permite por medio de las lectoras ubicadas en los diversos portales y que pueden operar de manera stand alone, el acceso a los portales correspondientes.
- Desde el punto de vista de seguridad el esquema controlado por un computador Central ofrece una ventaja adicional y es que en un instante se suprime o cambia el acceso a determinadas áreas a una persona o grupo de personas, en caso de extravió, simplemente anulando el código de acceso la entrada se restringe, para ello sólo debemos hacer un simple cambio en la base de datos

5.1.4 Técnicas de Codificación para Sistemas Portables. Existe una amplia variedad de técnicas y tecnologías que se utilizan para la codificación de las tarjetas de acceso. Al principio las primeras tarjetas iban de la mano con la tecnología existente de sistemas tales como tarjetas perforadas y tarjetas con códigos de barras, pero en la medida que los sistemas de control de acceso fueron creciendo para convertirse en una

industria floreciente, así como con los nuevos requerimientos de seguridad, nuevas generaciones de control de acceso fueron apareciendo.
En la actualidad podemos resumir en una media docena de esquemas diferentes los que hay en el mercado y la mayoría de ellos utilizan alguna forma de magnetismo para la grabación de los códigos.
Para criterio de estudio dividiremos la metodología de codificación en:

- Métodos Simples, son aquellos que se derivan de las primeras generaciones, tarjeta perforada.
- Embedded System, que constituyen la segunda generación de sistemas de Control de Acceso, siendo los más difundidos en la actualidad, Tarjeta Magnética, Tarjeta Wiegand, Tarjeta de Proximidad.
- Sistemas Biométricos y Tarjetas Inteligentes constituyen la nueva generación de Control de Acceso. *Dado que la tarjeta Inteligente se ha impuesto como estándar en la institución obviaremos las otras tecnologías de avanzada, aunque recomendamos su análisis. Desde nuestro punto de vista nos inclinamos a la tecnología Biométrica, si se utiliza sólo como Control de Acceso.*

5.2 Tarjetas Inteligentes Las tarjetas inteligentes, o Smart Card (tarjetas chip) nacieron en el año 1983. Su filosofía es muy sencilla, se trata de almacenar información con una cierta autonomía. Aunque la cantidad de información que pueden almacenar es relativamente pequeña, su autonomía es lo suficientemente importante como para haber producido la expansión de este tipo de tarjetas en el mercado.
La tarjeta inteligente es básicamente un chip, encapsulado en un rectángulo de PVC de aproximadamente 85′ 54 mm. Las tarjetas se suministran habitualmente en color blanco, pero pueden ser impresas utilizando diferentes sistemas. El chip que contiene dispone de unos contactos exteriores que son los que le permiten mantener una comunicación con él, y de esta forma acceder a la información que contiene o grabar nueva información. Estos contactos están bañados en oro para que la tarjeta sea resistente a un uso habitual en cualquier tipo de entorno (alta humedad incluso con condensación, ambientes químicos,...). Su pequeño formato hace que sea ideal como sistema de identificación personal. Además, su medida no está limitada por razones técnicas, sino por razones de estandarización, es decir, técnicamente se podrían utilizar tarjetas que fuesen la cuarta parte de las actuales. En el **anexo 4**, podemos determinar de manera más detallada todo lo relacionado con este esquema de seguridad.

5.2.1 Experiencia Es evidente que su uso está probado y la expansión realizada por estas tarjetas al nivel de tarjetas monedero, telefónicas y sistemas de almacenamiento de información sanitaria, tanto en Francia como en Estados Unidos, son muestras de su utilidad y fiabilidad. Otra ventaja de adoptar este sistema es el hecho del continuo aumento del uso de estas tarjetas por parte de los usuarios. Los beneficios que reporta el uso de las tarjetas inteligentes en el entorno de tarjetas monedero son obvios, sino fuera así no hubieran adoptado este sistema ni la Banca ni las grandes multinacionales. Evidentemente, el negocio está en disponer anticipadamente de un capital para cubrir el coste de unos servicios que aún no se han prestado. Esto supone unas ventajas tangibles para el empresario desde el punto de vista de financiación, previsión de gastos, e incluso de disponibilidad de capital para inversiones.

5.2.2 Aplicaciones La realización de software asociado a este nuevo entorno permite diversidad de aplicaciones comerciales. Sin embargo actualmente no existen demasiados equipos de desarrollo que trabajen en esta línea debido a la poca expansión del sistema y a la gran tecnología requerida. Aplicaciones tipo con tarjetas inteligentes son:

- **Control de acceso y de presencia**. Limitan y controlan el acceso a áreas restringidas, edificios, oficinas, clubes, administración, computadores, etc.
- **Pagos electrónicos**. Ofrece una solución ideal para aplicaciones de tarjeta monedero, tarjetas telefónicas, maquinas expendedoras, clubes de clientes, compras electrónicas, ...
- **Transportes**. Medio de pago seguro y fácil de utilizar para transportes públicos, billetes de avión parquímetros, peajes de autopistas, ...
- **Identificación y seguridad en informática**. Control de acceso a computadores, terminales, redes, aplicaciones de software, bases de datos, directorios, archivos confidenciales, ...

- **Sanidad**. Almacenamiento de los datos del paciente, incluyendo su historial médico. Para que los profesionales sanitarios puedan utilizarlos.
- **Procesos industriales**. Control de accesos en procesos de producción, medición de tiempos, seguridad industrial, ...

5.3 Control Perimetral CCTV el concepto de fortaleza es la base para el Control Perimetral y la defensa debe hacerse sobre la base de edificaciones concéntricas con áreas interiores destinadas a la ubicación de los equipos críticos, bajo el concepto de fortaleza, este concepto debe incluir las paredes de la edificación, las áreas donde están ubicados los equipos críticos y los gabinetes donde dichos equipos reposan. Los centros de computo de la institución no están ubicados en edificios especialmente diseñados para ello, sin embargo la recomendación es que estén ubicados lo más cerca posible de la planta baja, que no posean ninguna ventana y que no exista ninguna pared que dé a la parte externa del edificio, esto quiere decir que dichos centros deberían estar situados en áreas internas, rodeados por oficinas que dan a la parte externa, las paredes de dichos centros deben ser recubiertas con productos antifuego y aislantes y se tratará en lo posible de eliminar toda comunicación externa por ductos, tuberías, etc. A fin de evitar la propagación exterior de incendios o calor.
Las funciones de Control Perimetral son: **disuasión, retraso, discriminación y detención.** Los tres primeros los trataremos bajo el concepto de Control Perimetral, Discriminación debe ser tratado bajo el concepto de Control de Acceso.
Un segundo elemento de los tres mayores ingredientes de un sistema de seguridad (acceso, CCTV y alarmas) **CCTV** o Circuito Cerrado de Televisión realiza dos funciones principales, permite a una persona observar lo que esta sucediendo sin necesidad de estar presente y grabar las escenas para uso en el futuro, sin tener necesidad de que la persona este presente para llevar a cabo esta acción. La primera función es utilizada ampliamente por diversos negocios para vigilar áreas remotas que no están atendidas de esta manera pueden ser detectadas la presencia de intrusos o cualquier problema que pueda presentarse, además de lo anterior mencionado estos equipos actúan como disuasivos. Estos sistemas tienen la particularidad de integrarse con el del control de acceso y el de alarmas de manera que desde una consola central se puede supervisar todo lo que sucede en el perímetro de la empresa.

5.3.1 Componentes existen una gran variedad de equipos CCTV, para ser usadas en una gran gama de ambientes y para un abanico de aplicaciones, las cámaras con gran angular pueden cubrir por completo una sala de computación, con lente zoom, puede enfocarse para dar un closeup de un determinado equipo, existen cámaras para ser usadas durante el día o de noche, cámaras para proteger áreas donde una chispa estática pudiera causar una explosión y cámaras para actuar en las peores condiciones ambientales además de las cámaras los otros componentes que debemos tomar en consideración al momento de seleccionar un equipo de CCTV son:

- Lentes.
- Monitores y consolas.
- Controles.
- Equipos de comunicación.
- Equipos de grabación.
- Equipos especiales para integrar al sistema único de vigilancia.
- Software de integración.

5.4 Alarmas debido a la naturaleza crítica de la información y el objetivo trazado desde un principio, *disponibilidad y confiabilidad* es nuestro deber buscar la manera de eliminar las causas que pueden producir el cese del servicio, una de las principales causas son las condiciones ambientales, por ello es básico predecir y prevenir los problemas antes de que los mismos acontezcan, dado que el número de áreas que deben ser protegidas son muy extensas, en muchos casos son centros no atendidos en todas las horas de servicio y aun las atendidas tienen una serie de áreas críticas a las que no puede hacérsele permanente seguimiento, se recomienda instalar alarmas que a su vez deben ser monitoreadas desde locaciones centralizadas que permitan tomar acciones al presentarse algún tipo de problemas, el monitoreo tendrá las siguientes características:

- Mostrará el estatus de cada instalación, con actualizaciones cada 30 segundos.
- Despliegue gráfico de áreas y anuncio audible de alarmas.
- Interrogación continúa.
- Notificación de fallas de hardware y Software.
- Monitoreo basándose en prioridades.
- Redundancia en componentes críticos.
- Capacidad de upgrade.
- Auto monitoreo.
- Procedimiento automático de escalamiento.
- Confiabilidad probada sobre el 99% de optimo funcionamiento, por al menos 4 meses de funcionamiento continuo.

Un esquema básico de Control de acceso debe monitorear el siguiente tipo de información:
- Control de acceso
- Control de inundaciones bajo piso falso
- Control de humedad
- Control de alarmas de incendio
- Control de temperaturas
- Control de movimientos de equipos
- Control de vibraciones
- Detección de mal funcionamiento de alarmas
- Detección de supresión de alarmas
- Sistema eléctrico
- UPS
- CCTV

5.4.1 Operación las alarmas centralizadas tendrán un punto único de operación desde donde se controlará y monitoreará, de igual manera se detectará el estado de los elementos críticos y se ubicará en la central de vigilancia de la institución, la idea es tener información en tiempo real que permite al oficial de guardia tomar acciones a distancia a fin de disminuir los riesgos que pudieran presentarse. En dicho centro a su vez reposará un documento de operación y acciones ante una emergencia, igualmente un manual con las políticas de escalabilidad en el tiempo y que se emplearán al momento de alarma o contingencia y que lógicamente estará integrado con el Plan de Contingencia de la institución.

5.5 Seguridad Ambiental en la medida que la disponibilidad de los equipos se ha incrementado llegando en muchos casos a una rata del 99%, la causa más común de que un equipo deje de actuar es la falla eléctrica. Afortunadamente la misma es fácilmente controlable.

5.5.1 Electricidad el servicio eléctrico y los alimentadores que sirven a los servicios de computación deben:
- Tener suficiente capacidad para sostener por encima del 125% del total de carga conectada.
- Los equipos deben estar aislados de equipos que puedan causar fallas de corriente transitorias.
- El servicio debe ser suplido por al menos dos fuentes de alimentación y puede usar para ello un Switche de transferencia

5.5.1.1 Esquema de Emergencia del Servicio Eléctrico es esencial tener un inventario completo de los equipos y el consumo de energía de los mismos, de igual manera debe identificar los equipos críticos y su carga para en caso de necesidad trabajar con el mínimo de energía requerida. Además debe buscar como elemento de seguridad y contingencia la siguiente disposición de equipos cuyo objetivo es reducir el impacto de una caída abrupta de la energía eléctrica, entre ellos cabe mencionar:
- *Flywheel* esto nos proporciona 15 segundos de energía desde el instante en que deja de producirse el fluido eléctrico, el mismo es un motor eléctrico conectado a la entrada de AC, el motor maneja un alternador que mantiene la electricidad en el centro por breve tiempo mientras arrancan los

equipos que suministraran la energía alterna, en la actualidad la mayoría de los equipos críticos como computadores y unidades de disco, lo tienen integrado

- *Un UPS Básico* el mismo debe estar en capacidad de suministrar la energía requerida por el centro por 45 minutos, esto será suficiente para que el personal complete los procesos y apague los equipos
- *UPS Modificado* es un UPS al que se le agrego un Switche de transferencia entre el UPS y la acometida de AC, con este equipo se produce la transferencia a la línea alterna y deja de operar el UPS si esta recibiendo el servicio de la nueva línea, una vez reconectado el servicio el Switche vuelve a la línea principal.
- *Planta Eléctrica de Emergencia* que sea capaz de suministrar energía por un tiempo razonable, cumple dos funciones: mantener el centro funcionando y recargar las baterías del UPS.

5.5.1.2 Reguladores no se debe permitir que existan fluctuaciones en el servicio de AC que estén por encima del 5% de las exigencias recomendadas por el suministrador del equipo, es por ello que debe tener un voltímetro digital para monitorear el flujo de corriente, el mismo debe ser capaz de responder a una fluctuación de un milisegundo, el mismo debe ser supervisado con cierta regularidad y de ser posible integrado al esquema automatizado de alarmas, el voltímetro nos suministra información muy interesante para la investigación de fallas y la determinación de intentos de penetración al discernir que una falla sólo se produjo en el área del centro permaneciendo el resto de los ambientes sin ningún tipo de problema.

5.5.1.3 Switche de Emergencia el Switche Maestro (que para los efectos es el Switche de Emergencia), controla todo el sistema del Centro de Cómputos. Por razones de seguridad deben ser dos: uno debe estar instalado cerca de la consola del Centro de Cómputos, mientras que el otro se ubica cercana a la puerta de acceso principal, debe estar claramente señalada su función y para poder interactuar con ellos debe ser requerido un pequeño esfuerzo. Se accionara de manera automática cuando la temperatura exceda los 30 grados o la humedad relativa varíe en un 40%, de igual manera debe actuarse si se presenta cualquier anomalía o combinación de anomalías que puedan afectar a los equipos o la integridad de la data que se encuentra almacenada, debe estar integrado al esquema automatizado de alarmas.

5.5.1.4 Suspensión de Interferencias campos magnéticos y electromagnéticos deben mantenerse por debajo de los mínimos aceptables, cuyo valor para campos electromagnéticos es 0.5 voltios Por metro medidos de acuerdo con los estándares de la IEEE, el campo magnético aceptado es aquel que muestra una fuerza de 50 oersteds. Una buena conexión a tierra reduce las interferencias electromagnéticas, igualmente es conveniente instalar filtros de radio frecuencia en el punto donde la instalación eléctrica entra al centro de computación. Los cables deben estar cubiertos, ello incluye líneas telefónicas y alarmas

5.5.2 Control de Polvo los periféricos que se encuentran dentro del Centro de Computación son afectados negativamente por el sucio y polvo que son producidos por el óxido emitido por las cintas magnéticas, el papel y sus restos producidos por las impresoras, por tanto deben ubicarse filtros que minimicen el efecto que este polvo deja, con frecuencia debe eliminarse el resto que queda ubicado bajo el piso falso.

5.5.3 Filtros de Aire deben instalarse filtros en los ductos que suplen aire al centro de computación, ellos deben estar formados por material no combustible, lo suficientemente amplios para cubrir las entradas de aire, y lo más importante, deben tener una frecuencia para su limpieza y reemplazo al momento que sea requerido, de acuerdo con las especificaciones del proveedor.

5.5.4 Temperatura la temperatura dentro del centro debe ser mantenida dentro de los límites recomendados por los productores de equipos, en general la temperatura debe estar alrededor de 22 grados Centígrados y su fluctuación no debe estar por encima o debajo de los 5 grados

5.5.5 Humedad la humedad debe estar controlada de acuerdo con las especificaciones del fabricante de los equipos, que usualmente está alrededor de 50% de RH con una fluctuación máxima del 10%, algunos

equipos son afectados negativamente por baja humedad que permite la acumulación de electricidad estática, una descarga estática puede borrar la memoria o quemar circuitos

5.5.6 Protección Física de los Ductos los ductos es una ruta fácil para los intrusos, y de hecho instituciones que manejan información muy crítica recomiendan que los ductos deben ser divididos si tienen grandes dimensiones y no deben exceder en su volumen al tamaño de una mano abierta. Para casos de protección anti incendios, especifica que el material con que se construyen los ductos debe estar hecho con material retardador del fuego.

5.5.7 Dampers deben estar preparados para cerrarse en caso de fuego utilizando para ello un mecanismo que actúe conjuntamente con la alarma de incendios

5.5.8 Aire Acondicionado el aire acondicionado que sirve al centro de computación, debe estar separado del aire que sirve al resto del edificio, la sala debe ser servida por al menos dos equipos independientes, de igual manera estos equipos deben ser alimentados con las precauciones señaladas al momento de hablar del flujo eléctrico para los equipos del centro, pero deben a su vez poseer un circuito independiente

5.5.9 Monitoreo Ambiental al menos dos monitores ambientales deben ser instalados, que permitan determinar la humedad relativa y la temperatura, estos controles deben tener un procedimiento especificado para su revisión y mantenimiento

5.6 Protección del Centro de Computación el centro y el área donde se almacenan los datos deben tener:

- Una cubierta retardadora para casos de incendio.
- Estar protegido por alarmas contra intrusos, incendios.
- Alarmas que detecten la sustracción de equipos e información de fácil movilidad.
- Las paredes deben ir de losa a losa, cubiertas con material no combustible y con retardadores.
- Los ductos de entrada y salida igualmente deben estar sellados.
- Al menos deben ubicarse dos salidas de emergencia.
- Si el acceso es llevado a cabo por equipos de control automático, esta entrada debe ser independiente de las salidas de emergencia, puesto que se corre el riesgo de que en caso de fuego estos equipos no funcionen satisfactoriamente.
- Dentro del centro de computación deben separarse los ambientes de impresión, grabado y operación.
- Tanto el Cielo raso como el piso falso deben estar construido por material no combustible, debe instalarse en ellos alarmas de incendio e inundación

5.7 El tiempo como factor de protección contra incendios en las facilidades del centro no sabemos en muchos casos lo que significa perder un minuto de procesamiento en línea para una empresa, pero conocemos lo que es perder un día o un mes.... Para los efectos de protección de la empresa y del centro una de las más importantes medidas viene dado por el tiempo que tardamos en reconocer o detectar la presencia del fuego. En esta época en la que el tiempo tiene más valor que el dinero, la continuidad operativa de la empresa es un riesgo y particularmente en el caso de fuego. Inclusive un pequeño incendio no detectado a tiempo puede dañar importantes equipos o destruir importante información. Por esta razón en los últimos 20 años los profesionales de sistemas han tenido que evaluar sistemas de protección contra incendios no sólo desde el punto de vista de costo y conveniencia, también en su evaluación tiene alta preponderancia su capacidad de detección y supresión rápidamente.

5.7.1 Halon 1301 antes de 1964 básicamente se utilizaban dos esquemas. El primero era un gas supresor de fuego ubicado convenientemente y activado por un esquema de detección de humo. Cuando más de un detector en cualquiera de las áreas protegidas sentía la presencia de humo, se enviaba una señal que activaba el sistema de supresión de incendios. El factor suspensor gaseoso se conocía como el Halon 1301, un gas no nocivo y que trabajaba perfectamente para cualquier tipo de incendios, no era conductor de la electricidad y posterior a su uso no se requería ningún tipo de limpieza adicional. Cuando esta integrado propiamente con un esquema detector que permita la liberación del gas, la supresión del incendio toma

menos de 2 minutos. Esta rápida respuesta no da la oportunidad de la expansión del fuego y por tanto el fuego esta circunscrito a un espacio muy pequeño.
Estos sistemas esta respaldado frecuentemente por un sistema de Sprinklers, que no se activa a no ser que la temperatura del aire alcance una temperatura superior a los 500 grados.
En el año 1994, las reglas de protección para centros de computación cambiaron radicalmente por el *Protocolo de Montreal* que prohibía el uso de ciertas sustancias que se había comprobado que afectaban la capa de Ozono y entre ellos se encontraba el Halon y por ello la convención de Montreal y los países signatarios decidieron el cese de su producción y la eliminación para el año 2002, como resultado de dicha resolución el Halon 1301 prácticamente ha desaparecido, obligando a los centros de computación a buscar alternativas para su protección contra incendios. Para ello se han dado tres pasos que suplen en cierta manera los procedimientos existentes

5.7.1.1 El primer paso es hacer un upgrade del sistema detector de incendios en el pasado los esquemas detectores tenían dos debilidades, la respuesta lenta al momento de la detección y el fastidio de las alarmas dado por falsos positivos. Para que el detector actué debe existir cierto nivel de humo que llegue a los detectores doquiera que se encuentren, además al menos dos detectores deben ser activados para que el extintor actué, como resultado de ello hay un lapso de tiempo precioso previo al proceso de extinción, si a ello agregamos el pobre mantenimiento que se le da a estos sistemas, las interferencias eléctricas que producen en muchos casos falsos positivos y el temor constante de que estos sistemas se disparen dejando eventualmente sin protección al centro. Afortunadamente el avance de la tecnología esta revolucionando la ciencia de la pronta detección de incendios, con dos recientes innovaciones:
La primera **HSSD** (high sensitive smoke Detection) este concepto emplea sofisticadas técnicas para tomar muestras de aire 1000 veces más sensibles que los esquemas anteriormente existentes y que aun hoy se venden en países donde la regulación o la falta de ella lo permiten, esto permite determinar situaciones de posible fuego antes de que aparezcan las llamas o el humo. Los sistemas HSSD son capaces de detectar niveles de partículas en combustión a una concentración del 0.003% por pie, en ese estado sólo existen productos invisibles de combustión tales como los gases de los componentes eléctricos, este incipiente estado es seguido posteriormente por el humo, la llama y finalmente el calor intenso. Dado que continuamente HSSD, esta tomando ejemplo en el aire, se pueden detectar partículas de combustión en su estado incipiente y de esta manera dar alarmas con mucha anticipación.
El segundo elemento en importancia en el proceso de detección lo constituyen los detectores análogos, construidos sobre microprocesadores que permiten distribuir la inteligencia de detección lo que hace al detector un elemento más inteligente al momento de detectar y tomar decisiones sin ir a paneles de control. Estos detectores inteligentes a su vez producen reportes con respecto a su uso interno. Estos detectores tienen tres mayores ventajas sobre otros equipos menos novedosos, el primero reduce el tiempo de comunicación y toma de decisiones lo que elimina la problemática de los falsos positivos, el segundo viene dado por la disponibilidad y la confiabilidad que viene dado por su propia capacidad de detección de fallas en el equipo, y el reemplazo de los equipos viejos por estos nuevos está eliminando cableado que trae como consecuencia disminución en costos y tiempo.
5.7.1.2 El segundo paso cambiar el sistema Halon 1301 todavía hay muchas instalaciones que utilizan Halon 1301 como protector de incendios, como dijimos anteriormente el Halon 1301 es un agente ideal, el no tiene color, ni olor, se encuentra compactado como líquido en un cilindro que al momento de descarga se transforma en gas, puede alcanzar cualquier espacio dentro del área de protección, lo que elimina cualquier resquicio de incendio incluyendo los de origen eléctrico, papel y líquidos inflamables. El Halon es seguro no afecta a las personas y lo que es más importantes no deja ningún tipo de residuos. Convencionalmente un sistema Halon consiste de uno o varios cilindros con un sistema propulsor que les permite llegar a todos los puntos que se deseen proteger, este sistema reacciona eficientemente en caso de emergencia descargando la totalidad del agente en el lapso de 10 segundos, suspendiendo el fuego de manera rápida y eficiente. Pero dada todas las ventajas que hemos venido hablando alrededor del Halon, su reemplazo no puede ser un atraso y en esa investigación se ha llegado a dos agentes que químicamente son muy parecidos, ellos son **FM-200 y HFC-227ea,** son agentes gaseosos muy similares a Halon 1301 y extremadamente efectivos en incendios clase A, B, C, a diferencia del Halon 1301, que actúa por

interferencia con el proceso de combustión, estos productos producen una reacción endotérmica que absorbe el calor.
Ambos agentes no son conductores eléctricos, seguro para las personas y no requiere de limpieza adicional después de su propulsión, no tienen ninguna acción sobre la capa de Ozono y adicionalmente a lo anteriormente expresado los cilindros que contienen Halon 1301, pueden ser llenados con estas sustancias haciendo pequeñas modificaciones en el sistema propulsor
5.7.1.3 El tercer paso detección y supresión en un solo sistema finalmente pensemos en un esquema de Total Protección contra Incendios (TFP), esto quiere decir que el propio sistema cumple con cuatro funciones que son: detección, alarma, control y supresión. Estas funciones generalmente estaban separadas. Para ello busquemos una solución que comience con HSSD de detección inteligente lo que nos proporciona por su pronta capacidad de detección del tiempo para analizar la situación, alertar al personal, apagar los equipos, eliminar la fuente del fuego y controlar la activación del sistema de supresión

5.8 Daños Estructurales Daños estructurales a las áreas que ocupan los centros de computo o donde se procesan servicios, tienen diversas formas de materializarse: un terremoto, efectos del viento y huracanes, tempestades, avalanchas o daños intencionales o no realizados con estructuras pesadas (camiones, autos, aviones?), También pueden producirse como consecuencia de daños ocasionados a estructuras en los alrededores. Algunas estructuras son más propensas a daños que otras, aquellas ubicadas en áreas propensas a terremotos, equipos pequeños como los microcomputadores y pequeños servidores o equipos ubicados en salas de cableado son más propensos a sufrir accidentes.
La prevención de este tipo de accidente básicamente corresponde a un problema de Ingeniería estructural, pero en todo caso debemos tomar ciertas medidas básicas como sería la ubicación de los equipos en un edificio, es ilógico que como sucede en Caracas en edificios propensos a inundaciones el Centro de Cómputos se ubique en el sótano

Capítulo VI

Acceso

6 Autenticación y Encriptación la Autenticación es el proceso por medio del cual ambos extremos de la conexión se identifican y de forma cierta especifican quienes son. La Encriptación nos ayuda a asegurar que la información que se accede mientras dura la sesión no se encuentra comprometida. Lo que implica no sólo un tercero pueda leer los registros, también supone su alteración

6.1 Las necesidades de mejorar la seguridad cuando la versión 4.0 de IP, que en la mayoría de los casos hoy se sigue usando se creo eran los finales de los 70's y la seguridad de las redes no era la principal preocupación de quienes lo crearon, aunque ya en aquella época era importante la seguridad de los sistemas muy poca importancia se prestaba al transporte de la información, por tanto al introducirse IP, no presto ninguna importancia al esquema de protección y en las especificaciones de IP no se toma en cuenta que alguien deseara proteger la data que se esta transportando. Esto cambia con la versión 6, pero aparentemente la aceptación de esta nueva versión aun tomara algún tiempo

6.1.1Texto Limpio (Clear Text) actualmente la información transmitida por IP, se hace de una manera limpia, lo que implica que la información mana tal cual se genera

6.1.2 Monitoreo del Texto limpio capturar la información emitida por un texto limpio resulta una tarea muy sencilla, para ello se requiere sólo de un Network Analizer que puede ser una herramienta de hardware o un programa de software que corre sobre un sistema existente, su costo es de alrededor de $ 1000.00 para plataformas Windows o MAC (Media Access Control), siendo libre de cargo para estructuras UNIX, estos equipos operan como elementos pasivos, lo que indica que no requieren enviar ningún tipo de aviso cuando están monitoreando un equipo, de hecho ni siquiera requieren de una dirección de IP, lo que nos indica claramente que podemos tener un equipo analizador de datos en la red funcionando y no darnos cuenta de ello. Para capturar la información un Data Analizer, simplemente debe ubicarse en algún punto del camino por donde pasan los datos, esto quiere decir, en cualquier punto de la red entre el inicializador de la sesión y el punto de destino.
Entre los protocolos que transmiten en forma de Clear Text, entre otros podríamos mencionar:

- FTP la autenticación es Clear Text
- Telnet.. la autenticación es Clear Text
- SMTP... La contestación de los mensajes es Clear Text
- http... la información en toda su extensión es Clear Text
- IMAP... la autenticación es Clear Text
- SNMPv1... la autenticación es Clear Text

6.2 Requerimiento de buena autenticación la necesidad de una buena autenticación suena obvia ya que algo que pasa la información en un texto limpio, puede ser fácil de monitorear, este problema se hace más crítico en ambientes en donde no se obliga el cambio frecuente de passwords, lo que da al atacante todo el tiempo necesario para: planificar y efectuar el ataque, si además utiliza el mismo logon y password para todas las cuentas esto es todavía más sencillo. Lo que quiere decir que si captura esta información de un servicio inseguro tal como lo es POP3 (Post Office Protocol), podemos hacer logon en cualquier aplicación que utilice el usuario. Una buena autenticación va más haya de validar que la fuente que esta accedió al hacer el login inicial continua siendo la misma a lo largo de la sesión.
En un reciente artículo producido por Gartner Group[6], obtenemos los siguientes resultados sobre una base de 1500 gerentes de Centros de Computación "los consumidores profesan un gran temor con respecto a la privacidad, pero hacen muy poco para protegerse", los resultados obtenidos son:

- 59.3% de los entrevistados usan el mismo password en todas sus aplicaciones

[6] Privacy and Security Enero 2002

- 13.4% cambian el password al menos 2 veces al año
- 35.6% se interesa por políticas de privacidad
- 32.3% permiten cookies
- 12% usan software anónimo
- 10.2% buscan de manera activa y leen información privada

6.3 El modelo convencional de Encriptación el proceso convencional de encriptación, sigue el siguiente proceso, mensaje original, denominado "Plaintext", es convertido mediante un proceso random en un lenguaje aparentemente sin sentido conocido como "Ciphertext". El proceso de encriptación consiste de un algoritmo y una clave. La clave *es el valor independiente del Plaintext* que controla el algoritmo y el producto es un valor diferente en su resultado, dependiendo de la clave especifica que sé este utilizando, por tanto *cambiando la clave alteramos la configuración del Ciphertext*. Una vez producido el Ciphertext, es transmitido y posterior a la recepción, el texto puede ser transformado a su versión original Plaintext usando el algoritmo de decriptación y la misma clave que se utilizo originalmente para el proceso original de encriptación. La seguridad de este tipo de encriptación depende de diversos factores siendo el primero de ellos el algoritmo de encriptación que utilizamos, por tanto dicho algoritmo debe tener suficiente fortaleza que dificulte en grado extremo el descifrar el mensaje basándose para ello en el Ciphertext. Pero para lograr esto depende básicamente de la clave y debemos mantenerla en secreto. No requerimos que el algoritmo sea un secreto, por tanto el conocimiento del Ciphertext y el algoritmo para encriptar no es suficiente para la obtención del Plaintext, por lo anterior deducimos que *el secreto y el éxito consisten en no revelar la clave utilizada*. Este efecto es lo que hace que este método se dispersara rápidamente y ha hecho fácil a los manufacturadores el desarrollo de los chips a un muy bajo costo que permite encriptar la información. Si tomamos una versión más cercana del esquema convencional de encriptación, tendremos que existe un mensaje original que esta en Plaintext $\mathbf{X= [x_1, x_2, x_3...., x_m]}$ los M elementos de X son letras que pertenecen a un alfabeto finito, este alfabeto básicamente consta de 26 letras. Para efectos de encriptación la clave **K**, se expresa como $\mathbf{K= [k_1, k_2, k_3,..., k_j]}$, la misma es generada por el algoritmo y es proporcionada al destinatario por medio de un canal seguro o como medida alterna, una tercera parte podría generar esta clave y remitirlo tanto al originador como al destinatario. Con el mensaje **X** y la clave de encriptación **K** como entradas, el algoritmo forma el Ciphertext $\mathbf{Y= [y_1, y_2, y_3,..., y_n]}$ que podemos referir como $\mathbf{Y=E_k(X)}$. Esta notación indica que **Y** es producida utilizando el algoritmo de encriptación **E** como una función de Plaintext **X** y la función específica es determinada por el valor de **K.** El que recibe el mensaje que está en posesión de la clave puede invertir el Ciphertext utilizando la función $\mathbf{X=D_k(Y)}$.
Pero un observador que no tenga acceso a **K o X** debe intentar la recepción de uno de ellos o de ambos. Si asumimos que el oponente no conoce ni **E ni D**. Si el oponente esta sólo interesado en el mensaje específico, enfocará su esfuerzo a recuperar **X**, para ello genera un Plaintext estimado $\mathbf{\hat{X}}$, pero si su objetivo es poder descifrar toda información mandada, en ese caso debe generar un estimado de **K,** que llamaremos $\mathbf{\hat{K}}$. La *figura 6.2* muestra gráficamente lo que hemos expresado

6.3.1 Clasificación de los Sistemas Criptográficos los sistemas criptográficos son generalmente clasificados basados en tres dimensiones independientes:

- **El tipo de operación** usada para transformar el Plaintext a Ciphertext, estos algoritmos en forma general se basan en dos principios **sustitución** en el que cada elemento del Plaintext (bit, letra, grupo de bits o letras) son transformados en otros elementos, y la **trasposición.** Pero con la precaución de que en dicho proceso no se pierda la información
- **Número de claves** sí tanto el remitente como el receptor usan la misma clave, se lo conoce como **Simétrico** que a su vez pude ser dividido en clave sencilla, clave secreta, o encriptación convencional. Si el que transmite y el que recibe utilizan diferentes claves, se los conoce como **Asimétricos,** que a su vez se dividen en doble clave o clave pública
- **Forma de ser procesado** puede ser por string de datos, también conocido como cifrado corriente o por bloques

6.3.2 Cifrado Corriente es uno de los métodos más simples de encriptación, cuando se utiliza este procedimiento cada bit de la data es secuencialmente encriptado utilizando un bit de la clave, si se utiliza siempre la misma clave de encriptación, a la larga parece fácil deducir al comparar diversos textos la clave,

por esta razón se utilizan diversas claves de longitud diferente y lo que ha logrado dificultar aun más su deducción es la generación random de la clave de encriptación. Este proceso de cambio continuo de la clave de encriptación es conocido como *one-time pad*

6.3.3 Cifrado de Bloque a diferencia del anterior en este caso se toman bloques de datos de un tamaño específico, la especificación del bloque de cifrado identifica que cantidad de dato debe ser encriptado en cada pasada así como el tamaño de la clave que se aplicará a cada bloque. Por ejemplo el Data Encryption Standard (DES) especifica que los bloques de datos son de 64 bits y la clave de encriptación es de 56 bits. Existe un gran número de algoritmos que pueden ser usados para el cifrado en bloque, el más simple es tomar la data y dividirla en bloques y aplicar la clave a cada uno de ellos, aunque el método es eficiente, el podría producir un Ciphertext repetido si dos bloques de data contienen exactamente la misma información. Para evitar esto y que se pueda quebrar con facilidad el algoritmo, se utiliza un proceso similar al presentado en el grafico que observamos a continuación Para ello se toman los resultados del algoritmo combinando con las claves. La información que se desea encriptar es dividida en bloques que identificamos DB1 a DB4, un vector de inicialización que identificamos como IV, que agregamos al principio del proceso para asegurara que todos los bloques estén propiamente cifrados, IV es simplemente un carácter randon lo que asegura que dos mensajes idénticos no produzcan el mismo resultado. Para crear el primer bloque de Ciphertext matemáticamente combina la clave de encriptación con el primer bloque DB1 con el vector de inicio IV.

6.3.4 Debilidades de la encriptación las debilidades pueden caer dentro de estas categorías

- **Descuido o Error Humano** algunos métodos de encriptación por si mismos pueden poseer procesos mejores o peores de encriptación, es por esta razón que cuando decidimos encriptar debemos asegurarnos poseer la infraestructura adecuada para administrar las claves de encriptación de una manera adecuada, alertando a las personas de la importancia que tiene para el proceso mantener la privacidad de la clave o password
- **Deficiencias en el Proceso** la determinación de deficiencias en el algoritmo de encriptación, es probablemente la tarea que seguirá cualquier persona que desee descifrar un mensaje, por tanto hay una serie de precauciones que deben seguirse para asegurar que el proceso es seguro. La fórmula matemática que conforma el algoritmo de encriptación debería ser de público conocimiento. El algoritmo de encriptación debe ser conocido de manera que pueda ser evaluado y discutido por sus seguidores. El algoritmo de encriptación debe ser público y disponible por un tiempo razonable de tiempo a fin de asegurarse que se pueda hacer un análisis minucioso del proceso antes de lograr su implantación.
- **Ataques por la fuerza bruta** este ataque es simplemente un intento, utilizando todos los recursos a la disposición de poder romper o determinar las llaves que permiten descifrar la información. Para llevar a cabo este proceso se evalúan todos los medios de romper la clave de encriptación en un tiempo razonable. Todo algoritmo de encriptación son vulnerables a un ataque por la fuerza bruta. En este proceso hay dos elementos que deben ser revisados con detenimiento el primero es *razonable* el atacante debe sentir que lanzar este ataque es perder el tiempo, para ello debemos tomar en cuenta el valor de la información que se quiere descifrar. La otra información es *vulnerable* aunque todo algoritmo puede ser determinado a través de un proceso de fuerza bruta, algunos toman exceso de tiempo y recursos para lograrlo y para el valor de la información que se quiere descifrar no vale la pena el esfuerzo. Por tanto el tiempo requerido para llevar a cabo este tipo de ataques debe tomar en cuenta dos factores cuanto tiempo perse tomara en lograrlo y cuantas combinaciones posibles tiene la clave que desea descifrar, en la tabla a continuación puede verse esta ultima variable

Software	Bits	Combinaciones
Netscape	40	1.1*10**6
DES	56	72.1*10**6
T DES 2K	112	4.2*10**33
RC4/128	128	3.4*10**38
T DES 3K	168	3.7*10**77
Futuro STD	256	1.2*10*77

La cantidad de tiempo requerido para determinar la combinación que se viene utilizando depende del poder del equipo que se esta utilizando, a manera de ejemplo un equipo de computación personal es capaz de probar 5 claves por Segundo, mientras que un equipo especialmente diseñado para detección de claves procesa 200. En los últimos años los laboratorios RAS ha sometido un reto para descifrar la información contenida en un texto. En el año 1997 el reto se completó, tomando para ello 5 meses, en Enero de 1998, tomó 39 días y en Julio de 1998 tomó 3 días, el costo del equipo utilizado para lograr esto fue de $250000 y la clave de encriptación descifrada fue la de Netscape(DES a 56 bits)

6.4 Autenticación Kerberos es una solución muy popular de autenticación, diseñado para Single Sign-on en ambientes heterogéneos, permite la autenticación y la comunicación encriptada entre los usuarios y los servicios a los que tienen acceso se puede conseguir en versiones gratis en Internet. Kerberos viene a resolver muchos de los problemas que se presentan en redes heterogéneas e incluyen la autenticación mutua entre el cliente y el servidor. La idea básica detrás de Kerberos está en que una tercera parte certifique la autenticidad (Servidor de Seguridad Kerberos). Kerberos ofrece además privacidad e integridad de la información. En una concepción básica Kerberos trabaja de la siguiente manera:

1. Un programa cliente ubicado en la estación del usuario, certifica su identidad contra el servidor Kerberos y lo verifica localmente en la estación de trabajo
2. El cliente Kerberos en la estación de trabajo, pide al servidor las credenciales necesarias, es decir exige su autenticación para usar los servicios a los que tiene acceso
3. El servidor Kerberos envía las credenciales al usuario
4. Una aplicación del cliente en la estación de trabajo, toma las credenciales de la memoria para que el usuario la presente al servidor de aplicaciones
5. El servidor de aplicaciones autentica la aplicación del cliente para el servicio que ha requerido y el servidor libera su uso.

Entre los servicios que Kerberos puede suministrar, caben mencionar Canales seguros, Integridad, Confidencialidad, Autenticación, Control de acceso, Disponibilidad, no-repudiación.

6.4.1 Intercambio Inicial Kerberos este proceso sigue los siguientes pasos:

1. La estación del cliente, inicializa el ambiente Kerberos corriendo un programa
2. El programa de inicio "KINIT", envía al Server de autenticación(AS) su ID
3. Las credenciales de AS, contiene el ID del cliente, la hora, y la clave de los servicios que puede utilizar, comprobado el ID, toda la información anterior es encriptada y se envía al cliente un TGT(Ticket Granting Ticket)
4. El programa "KINIT" pide al usuario que dé el password
5. Si el password es correcto el TGT es salvado en la memoria de la estación del cliente

6.4.2 Vulnerabilidades de Kerberos al igual que cualquier esquema de autenticación, Kerberos tiene ciertas debilidades. El diseño de Kerberos asume que el servidor principal mantiene áreas donde existe un moderado esquema de seguridad, que en el Key Distribution Center sólo corre software confiable, esto incluye previsiones de boot desde servidores igualmente confiables y la no-existencia de software de aplicación en las estaciones de trabajo. En un ambiente ideal, los discos se limpian después de tomar acción

un proceso de boot para asegurar que los efectos posteriores que pudiera tener un software infectado no afecten a los usuarios.
En este ambiente ideal tendríamos igualmente que indagar por la protección de la estación de trabajo. Como podernos asegurar que alguien no pueda acceder al password a través de mecanismos ocultos, lo que supone por supuesto una protección adicional a las estaciones de trabajo y una permanente auditoria a fin de asegurarnos que la misma no ha sido accedida por extraños
Como el Kerberos Key Distribution Center (KDC) contiene todos los secretos para proveer la seguridad, este debe ser protegido de una manera cuidadosa en extremo, aunque las estaciones no tengan toda la protección necesaria y los servidores no sean todo lo confiable que idealmente se requiera, el KDC debe ser 100% confiable, esto significa que todos los accesos al KDC deben ser cuidadosamente controlados y monitoreados. El KDC sólo debería soportar aplicaciones específicas de Kerberos, idealmente este sistema no soportaría acceso remoto, pero, si el KDC es administrado de manera remota, la operación debe hacerse a través de un canal seguro.
Si el KDC se ve comprometido, los secretos que mantenía el esquema de seguridad perderán toda su confiabilidad, pero debemos suponer que ese tipo de ataque esta lejos de ser fácilmente llevado a cabo. Kerberos usa DES para las operaciones de encriptación, todo el KDC es encriptado usando una clave maestra, por tanto para llevar a cabo un ataque al KDC el intruso debe poder acceder al KDC o en su defecto obtener una copia de su base de datos, lo que implicaría en todo caso lograr descifrar la información que está contenida en la base de datos aspecto que no es imposible pero tal como hemos visto implica un alto costo computacional poder romperlo.

6.5 Single Password Kerberos, da la facilidad de Single Sign-On, con la ventaja de que es gratis, y que con la nueva configuración del Sistema Operativo XP de Microsoft, ha tomado un excelente impulso. En su concepto más elemental puede ser definido como el proceso de minimizar el número de User Ids y passwords requeridos para acceder a varios sistemas en un ambiente de computación distribuida. En su más pura concepción sería el proceso por medio del cual al ingresar un usuario a la red conjuntamente con su ID y su password, se le garantiza el acceso a todos los ambientes y recursos requeridos para su trabajo y en su diseño es la herramienta que permite el cumplimiento general de las políticas de la institución, tal como lo mostramos en el capítulo II

6.6 Tokens también llamadas Tokens Cards son tarjetas generadoras de passwords que permiten acceder a los servicios tanto a clientes locales como remotos. Físicamente son tarjetas con una pequeña pantalla LCD, que muestra el password y el tiempo remanente para que el password expire, una vez que este tiempo ha pasado se genera un nuevo password, lo que proporciona un alto nivel de seguridad en el proceso de autenticación, para su funcionamiento requiere de un agente que sincroniza los passwords entre el usuario y el servidor que permite el acceso. Cada Token posee un número de seguridad, que identifica el Token con el servidor e identifica el algoritmo que usa el Token para generar el password por lo que diferentes Tokens generaran password diferentes

6.7 Conclusión el proceso de seguridad supone una serie de pasos que presentaremos en las conclusiones de este trabajo, pero para los efectos de conclusión de este capítulo, presentare una serie de etapas que nos permitan completar el trabajo requerido para poder cumplir con las políticas de seguridad establecidas ellas son:

1. De acuerdo con la sensibilidad de la información todo archivo considerado como confidencial será encriptado, y utilizará la tecnología de clave pública, siempre que sea requerido se usará la firma digital, utilizando para ello certificadoras tal como lo prevé la "Ley Sobre Mensajes da Datos y Firmas Electrónicas" de la República, en su articulado 9 y 14, referentes a la forma, 16 a 20, referentes a las firmas electrónicas y 31 referente a los Proveedores de los Servicios de Certificación. ver **Anexo 5**
2. Entre los productos de Single Sign-on existentes(Kerberos, MyNet, AutoSecure, Okiok, Securpass), seleccionar el que sea más expedito y nos permita hacer cumplir con los requerimientos establecidos por la política de seguridad

3. Dado que la tarjeta inteligente será el medio que utilizará la institución como control de acceso, evaluar la integración de la lectora a los equipos que manejan información crítica, como esquema de Control de Acceso
4. Para acceso desde áreas externas debe hacerse utilizando la tecnología de Tokens, tal como lo mostramos en el **Anexo 5**

Capítulo VII

Redes

7.1 Generalidades la seguridad de las redes van de la mano con la seguridad del computador, y hoy por hoy es extremadamente difícil separar una de otra. Actualmente todo desde las llaves electrónicas que nos permiten acceder a nuestro cuarto en un hotel, pasando por los teléfonos celulares a las laptops, están de una manera u otra interconectado a través de una red. Pero si bien las redes se han convertido en algo imprescindible, también es cierto que las mismas son muy inseguras. Es imposible que hablemos de Seguridad Computacional sin hablar acerca de Seguridad de Redes puesto que de una manera u otra los diferentes equipos electrónicos inteligentes, estarán interconectados. Las Redes o Computer Networks, no son más que grupos de computadores interconectados entre sí, cuando un computador desea hablar con otro crea un mensaje conocido como Packet o paquete, que tiene la dirección del computador de destino además de otra información de control y lo manda a través de la red. Estos paquetes que contienen todo tipo de información desde mensajes E-Mail, o GIFs con pornografía, tal vez audio o vídeo, o quizás una conversación telefónica, cualquiera sea la información que transporte, se descompone en pequeños paquetes que son enviados a la dirección de destino siguiendo cada uno de ellos rumbos diversos en el caso de la comunicación "no orientada a conexión", pero llegando al mismo sitio, donde se reensamblan y son recibidos tal cual su versión original. Estos paquetes son enviados a través de la red por medio de Routers, capaces de manejar diversos tipos de protocolos y que se encargan de revisar la dirección que trae consigo el Packet y enviarlo camino de su destino final.

7.2 Hardware básico de redes actualmente existe un sinnúmero de productos de redes que deben tenerse en cuenta al momento de planificar la infraestructura requerida. Hay equipos para caso todo desde la conexión de equipos de computación a la red al control de tráfico de la red.

- *Hubs* son probablemente los equipos conjuntamente con las tarjetas de red más usados. Físicamente son cajas de variados tamaños que presentan múltiples hembras de cable tipo RJ45, a través de cables al Hub se conecta un servidor o estación de trabajo. En esencia los Hubs son repetidores de multipuertos que soportan pares de cables en una topología de estrella, cada nodo se comunica con el Hub, el cual por turnos amplifica la señal y la transmite por difusión al correspondiente puerto, al diseñar su red piense en Hub como un equipo que no ejerce ningún control sobre el tráfico y funciona de manera similar a un repetidor.
- *Bridges* externamente se ven como un repetidor, es una caja pequeña con dos conectores que conectan dos porciones de la red. El incorpora las características de los Repeaters, pero actúa sobre los Frames de los datos los cuales son los más beneficiados. El Bridge utiliza los Frames de información para determinar el origen y destino de la información a través de las direcciones de MAC(Media Access Control) que posee cada Frame de datos, monitoreando esta información el Bridge conoce donde están ubicadas las redes, construye una tabla con las direcciones de MAC de los equipos sobre los cuales tiene acceso y utiliza esta información para regular el tráfico que pasa a través de la red y de esta manera puede regular dicho tráfico.
- *Switches* constituyen la unión de la tecnología de los Hubs y los Bridges, en apariencia son similares a los Hubs, tienen múltiples conexiones RJ45 por medio de los cuales conectan sistemas de redes. En vez de ser un amplificador sin inteligencia como sucede en el caso de los Hubs, el funciona como si internamente tuviera un Bridge en cada uno de sus puertos, el guarda información de las direcciones MAC de los equipos que están conectados a el con esta información el puede enrutar el tráfico destinado a cierta dirección únicamente al puerto al cual esta conectado. El Switche graba la dirección de identificación MAC de cada estación al enviar estas un Frame, actuando de esta manera similar a un Bridge. Varias cosas interesantes ocurren con esta situación, la primera es que cada cable enlaza la estación o el equipo con el Switche, lo que limita las colisiones únicamente a estos dos equipos, este elemento proporciona un gran rendimiento al aprovechar al máximo el ancho de banda, además de lo anterior también nos permite incrementar la seguridad ya que si alguno de los sistemas interconectados tiene problemas, estos sólo lo abarcan a el y no compromete al resto de la red. En algunos casos a los

Switches se les agrega un puerto de monitoreo, que es un puerto que puede ser configurado para monitorear la data transmitida y recibida por uno o varios puertos.

- *Routers* de acuerdo a los esquemas señalados por la Arquitectura Internet físicamente dos redes sólo se pueden conectar por medio de una computadora ubicada en medio de las dos. Además estas computadoras debe estar dispuesta a intercambiar paquetes de una red a otra. Estos equipos de interconexión y transferencia son conocidos como Routers. Que son más sofisticados y tienen capacidades no disponibles en los Bridges, siendo su principal característica la de poder seguir avanzando un mensaje, pero es importante saber que el Router no traduce protocolos de aplicación. Las principales aplicaciones de un Router son:
    - Control del Flujo si el camino que una información se encuentra congestionado él puede mantener dicha información mientras se despeja adelante el camino
    - Optimización de rutas el Router que transmite selecciona la ruta más despejada, para ello consulta en las tablas disponibles para obtener esta información
    - Secuencia los Routers envían la información en paquetes, estos llegan en desorden a su destino pero el Router que se encuentra al final de la vía conoce por la información que el paquete le suministra su correcto orden y arregla la información acorde con ello.
    - Acnowledgment el Router que recibe envía un mensaje al transmisor haciéndole conocer que la data ha sido recibida correctamente.

Un Router generalmente es un computador pequeño, con muy poca capacidad de almacenamiento y limitación en su memoria principal, como el ruteo esta basado en redes, la información que debe almacenar un Router es proporcional al número de redes dentro de otra red. La inteligencia inherente a un Router trae consigo dos desventajas, la primera es su instalación y mantenimiento, ya que debe mantener actualizadas sus tablas.

7.3 Seguridad de Bridges y Routers los Routers y bridges conjuntamente con los agentes de comunicación que conforman la capa 1, son los elementos básicos que comunican la información, por tanto una vez que una red es penetrada, la manera como se configuren estos equipos, determinaran hasta donde podrá el Hacker llegar, que equipos podrá atacar, en los esquemas de penetración una vez entrada en la red y tomando como base de ataque un servidor, el siguiente paso es apoderarnos de los Routers, si tenemos éxito la red nos pertenece en su totalidad, podremos subirla o bajarla, reprogramarla o simplemente cambiar el password del router, lo que traerá como consecuencia que el administrador de la red no tendrá acceso.

7.3.1 Bridge como dijimos anteriormente la función de un Bridge en la conexión es unir tramos de red, ello trae consigo una sensación de seguridad que muchas veces es engañosa y débil. Aunque las LAN asumen cierto grado de confianza en los usuarios de la red, a medida que esta crece, esta suposición va perdiendo validez y la seguridad se convierte en una cuestión fundamental. El hecho de que la mayor parte de las LAN sean de difusión implica que se pueda llevar a cabo fácilmente la escucha no autorizada de la información transmitida haciendo que la tarjeta NIC funcione de modo promiscuo, por el cual se capturan y examinan todas las tramas en la LAN. Al ampliar el número de usuarios los puentes tienden a incrementar este problema, sin embargo pueden también ayudar en el tema de seguridad dada su capacidad de *filtrar tramas*. A través del examen del contenido de las cabeceras de las tramas y los paquetes, los bridges pueden controlar el flujo del tráfico permitido desde y hacia un segmento dado de red. Es de hacer notar que en la institución se han presentado una serie de ataques por negación de servicio aprovechando la fragilidad que presenta la red

7.3.2 Routers en principio por el hecho de ser programables y tener dispositivos de seguridad le dan un criterio de mayor confiabilidad que la que el Bridge proporciona. Por medio de los ACL(Access Control List) son usados para limitar el tráfico entre diversos puntos en la red, en la institución es básico la revisión de los ACL, creemos que los mismos se muestran demasiado abiertos lo que facilita a cualquier persona que la quiera penetrar hacerlo con cierta facilidad como lo hemos llevado a cabo, pero por otro lado si la restringimos en exceso como ha sucedido últimamente tendremos que los usuarios no pueden en algunos casos acceder a su información o enviar transacciones a través de la red.

Existen dos tipos básicos de Routers los estáticos y dinámicos, los Routers estáticos usan las ACL para determinar si una data enviada es aceptada o rechazada ya que las ACL se pueden programar para cumplir con esa función, un router dinámico contiene una tabla con varias direcciones y las rutas que pueden seguirse para llegar a ellas, esto le permite en muchos casos acelerar el proceso de transmisión pues tiene rutas alternas para alcanzar un destino, estas rutas además son intercambiadas con otros Routers lo que incrementa la facilidad de acceso final al destino deseado ósea hablamos de limitación y overhead en el caso de estático, contra velocidad de acceso en caso de Routers dinámicos. Es básico desde el punto de vista de seguridad

7.4 Firewalls definiendo una política de acceso es simplemente una política corporativa que condiciona el tipo de acceso permitido dentro de los perímetros de su red, la misma aplica a las diferentes áreas que se desenvuelven dentro de la red. Una política de acceso simplemente define el flujo de datos desde y para las diferentes partes de la red, además especifica que tipo de tráfico es aceptable, asumiendo que aquel que no cumpla con esto es bloqueado. Cuando se define una política de acceso se tienen que utilizar una serie de parámetros para describir el flujo de datos. Entre los parámetros más usuales que deben ser descritos figuran:

- *Dirección:* da una descripción del flujo de datos basándose en una dirección, por ejemplo el tráfico desde Internet a la red interna(Inbound) o de la red interna a Internet (Outbound)
- *Servicio:* el tipo de servidor de aplicación que será accedido, por ejemplo Web Access(http), File Transfer Protocol(FTP), Simple Mail Transfer Protocol(SMTP)
- *Host Específico* algunas veces se requiere una especificidad mayor que la que expresa la dirección. Por ejemplo una organización puede tener tráfico Outbound pero sólo para un computador específico.
- *Usuarios Individuales* algunas organizaciones tienen individuos que llevan a cabo actividades específicas y no quieren que dichos privilegios se le den a todo el personal
- *Hora del día* algunas veces se requiere restringir la actividad durante ciertas horas, o durante ciertos días
- *Público o Privado* que tipo de red se usará para transmitir cierto tipo de información
- *Calidad del Servicio* algunas organizaciones tienen restringido el acceso a determinado ancho de banda.

Una política clara y bien definida de Control de Acceso le asegura que seleccionara el producto o productos de Firewall correctos, nada es peor que gastarse $ 10000.00 en un nuevo Firewall solamente para darnos cuenta que no cubre la necesidad que requeríamos.

7.4.1 Definiendo un Firewall un Firewall es un sistema o un grupo de sistemas que fuerzan el cumplimiento de una política de control de acceso, una vez que se ha determinado el nivel de conectividad que se desea suplir. El Firewall es similar a otros equipos que forman parte de la red en su propósito de dirigir el flujo de tráfico, pero a diferencia de otros debe tomar control sobre este tráfico, tomando en cuenta que no todos los grupos de datos son lo que aparentan. El Firewall no utiliza las reglas de comunicación como un soporte, el debe esperar que las reglas no se sigan, lo que pone gran presión en su diseño, que debe ser planeado para cualquier contingencia. Sin embargo en el diseño de las políticas debemos presuponer que las reglas en cuestión no serán cumplidas, lo que pone una excesiva presión en el diseño del Firewall, lo que nos lleva a sugerir la creación de esquemas de contingencia

7.4.2 Descripción de los Firewalls

- ✓ *Firewalls Como Filtros.*- El Router es un tipo especial de Switch el cual realiza el trabajo de hacer las conexiones externas y convertir el protocolo IP a protocolos de WAN y LAN. Los paquetes de datos transmitidos hacia Internet, desde un visualizador de un PC, pasarán a través de numerosos Router a lo largo del camino, cada uno de los cuales toma la decisión de hacia donde dirigir el trabajo. Los Router toman sus decisiones basándose en tablas de datos y reglas, por medio de filtros, así que, por ejemplo, solo datos de una cierta dirección pueden pasar a través del Router, esto transforma un Router que puede filtrar paquetes en un dispositivo de control de acceso o Firewall. Si el Router puede generar un

registro de accesos esto lo convierte en valioso dispositivo de seguridad. Si el servidor de Internet solicita información, o bien la suministra hacia sistemas de bases de datos distribuidas, entonces esta conexión entre el servidor y la estación de trabajo debería ser protegida.

- ✓ *Firewalls Como Gateway.*- Los Firewalls son comúnmente referidos como Gateways, controlan el acceso desde afuera hacia adentro y viceversa. Un Gateway es una computadora que proporciona servicio de intercambio de datos entre dos redes, un Firewall puede consistir en un poco más que un Router filtrador, como una Gateway controlada. El tráfico va hacia la Gateway, en vez de dirigirse directamente hacia la red, la Gateway que pasa los datos, de acuerdo a la política de control de los accesos, a través de un filtro, hacia otra red o hacia otra Gateway conectada a otra red. Esta mediación toma en cuenta, direcciones de fuente y destino, tipos de paquetes de datos, política de seguridad. Típicamente un Firewall registra los accesos y los intentos de acceso de una red a otra.
- ✓ *Firewalls Internos.*- Alguien fuera de la empresa podría solicitar cierta información, pero no necesariamente necesita acceder a toda la información interna. En estas circunstancias, los Firewalls juegan un importante papel forzando políticas de control de acceso entre redes confiables protegidas y redes que no son confiables En una WAN que debe ofrecer conexión de cualquier persona a cualquiera, otras formas en el nivel de aplicación pueden ser implementadas para proteger datos importantes. Sin embargo, separar las redes por medio de Firewalls reduce significativamente los riesgos del ataque de un Hacker desde adentro, esto es acceso no autorizado por usuarios autorizados. Agregando encriptación a los servicios del Firewall la convierte en una conexión Firewall a Firewall muy segura. Esto siempre permite redes grandes interconectadas por medio de Internet. Agregando autenticación se puede aumentar el nivel de seguridad. Por ejemplo una vendedor que necesite ver la base de datos de inventario, tendrá que comprobar que es él.

7.4.3 Características de Firewalls.- Los Firewalls de hoy tienden a combinar diferente mecanismos, haciendo difícil clasificarlos. Por esa razón se describen los ingredientes que pueden ir en el diseño de un Firewall.

- ✓ Filtrado de Paquetes.- Todos los Firewalls desempeñan algún tipo de filtrado de paquetes, comúnmente por medio de un Router de filtrado de paquetes. El Router filtra paquetes, haciendo que ellos pasen por el Router, implementando un conjunto de reglas con base en la política del Firewall. Un Router filtrador de paquetes, usualmente puede filtrar paquetes ip con base en algunos o todos los criterios siguientes:
  - ❖ Dirección fuente ip,
  - ❖ Dirección destino ip,
  - ❖ Puerto fuente tcp/udp, y
  - ❖ Puerto destino tcp/udp.

  El filtrado puede bloquear conexiones desde o a las redes o anfitriones específicos, y pueden bloquear conexiones a puertos específicos. Un sitio podría desear bloquear las conexiones desde ciertas direcciones, tales como desde anfitriones o los sitios consideraron hostiles o indignos de confianza. Alternativamente, un sitio puede desear bloquear conexiones desde todos las direcciones externas al sitio (con ciertas excepciones, tales como con smtp para recibir e-mail). Los servidores tales como el Telnet daemon usualmente reside en puertos conocidos (puerto 23 para Telnet), así si un Firewall puede bloquear conexiones tcp o udp a o desde puertos específicos, entonces el sitio puede hacer llamadas para asegurar los tipos de conexiones para ser hechas a ciertos anfitriones pero no a otros. Por ejemplo, una compañía podría desear bloquear todas las conexiones de entrada a todos los host a excepción a algunos sistemas conexos de Firewall. A esos sistemas, quizás sólo los servicios específicos serán permitidos, tal como SMTP para un sistema y conexiones Telnet o FTP a otro sistema. Con filtrado sobre puertos tcp o udp, esta política puede ser exitosa en este estilo de Router de filtrado de paquetes o un anfitrión con capacidad de filtrado de paquete. Algunos Router de filtración de paquetes no filtran en los puertos fuente tcp/udp, el cual puede hacer el filtrado más complejo el conjunto de reglas y pueden abrir hoyos en el esquema de filtración.

- ✓ Inspección de Paquetes.- Algunos Firewall de Internet combinan el filtrado de paquetes y el enfoque de aplicaciones Gateway, usando un filtrado de paquetes o un Router de hardware para controlar los niveles bajos de comunicación, y Gateway para habilitar aplicaciones. Esto puede crear un alto grado de control de acceso. Como siempre, esta adaptación puede limitar en transparencia, flexibilidad y conectividad, y puede también dar una mayor dificultad en términos de configuración, manejo y especialización. Otro punto de vista que gana aceptación es la inspección de paquetes que no solo los filtra, esto es, considerar su contenido tanto como sus direcciones. Los Firewall de este tipo emplean una inspección de módulos, aplicable a todos los protocolos que comprenden los datos de los paquetes destinados desde el nivel Network (ip) hasta el nivel de aplicación. Esta estrategia puede proveer seguridad sensitiva al contexto para complejas aplicaciones y puede ser más efectiva que la tecnología que sólo tiene acceso a los datos en ciertos niveles. Por ejemplo las aplicaciones Gateway sólo acceden a los datos de nivel aplicación, los Router tienen acceso sólo a niveles bajos, el enfoque de la inspección de paquetes integra toda la información reunida de todos los niveles en un simple punto de inspección. Algunos Firewall de inspección también toman en cuenta el estado de la conexión, por ejemplo, la legítima entrada de paquetes puede ser probada con la petición de salida para ese paquete y se le permite entrar. Por el contrario, un paquete de entrada se enmascara con su respuesta a una inexistente petición de salida, este será bloqueado. Esto lleva el enfoque de tan llamado estado (stateful) más allá del filtrado de paquetes. La inspección de módulos usa previas comunicaciones para derivar el estado actual de la comunicación que se esta realizando. El filtrado inteligente puede efectivamente combinarse con la habilidad del rastreo de la sesión de red. Para usar la información acerca del inicio y fin de la sesión en la decisión de filtrado. Esto es conocido como filtrando sesión (sesión filtering). Los filtros usan reglas inteligentes, así aumenta el proceso de filtrado y controlando el rastreo de sesiones de la Network que controla los paquetes individuales. Una sesión de Network contiene paquetes que van en dos direcciones, así que sin una sesión de filtrado cada sesión requiere dos reglas de filtrado de paquetes. La primera controla los paquetes que van desde el originario host hasta el destinatario host. Una regla inteligente, sobre la otra mano, sabemos que regresando el paquete dirigidos en sentido opuesto y así no necesitamos la segunda regla. Este enfoque ofrece ventajas considerables, desde los sitios que comúnmente tratan los paquetes originados afuera del Firewall de manera diferente que los paquetes que regresan desde una conexión autorizada afuera.
- ✓ *Firewalls Hibridos.*- En la práctica, muchos de los Firewalls comerciales de hoy usan una combinación de estas técnicas. Por ejemplo, un producto que se origino como un Firewall filtrador de paquetes puede haber sido mejorado con filtrado inteligente a un nivel de aplicación. Las aplicaciones Proxy en áreas establecida como FTP puede agregar una inspección de filtrado base en su esquema. Hay que recordar que, agregar los métodos de seguridad no significa necesariamente un aumento en la seguridad. Los mecanismos adicionales pueden aumentar, o disminuir la seguridad del Firewall.

7.4.4 Factores que no hacen deseable un Firewall

- ✓ *Ineficiente*: el Firewall se convierte en un cuello de botella de toda la estructura y debe poseer por lo tanto una eficiencia en la manipulación de los streams de paquetes igual o superior a la del Router que maneja tal enlace.
- ✓ *Poco seguro:* los Firewall son típicamente implementados en un sistema bajo un sistema operativo, que no necesariamente suministra la seguridad deseada y por tanto, los hace vulnerables, cuando se detecta una brecha, la misma es publicada y el administrador de la red no siempre se entera de dicha debilidad, por ello es el blanco típico de ataque para los programas especializados de scanning de los Hackers (estudian "pacientemente" múltiples opciones del sistema, hasta encontrar un punto de acceso o modificación). Si mi seguridad esta sustentada en una maquina cuyas debilidades son conocidas, entonces mi sistema no es realmente seguro. Muchas veces no son transparentes a la operación del usuario: debido a su diseño, algunos de estos modelos no son tan transparentes a la operación del sistema, complican la administración del sistema de comunicación (usualmente tienen interfaces de manejo propietarias). Algunos modelos basados en "Proxies" pueden ser muy seguros, pero algunos de ellos requieren versiones modificadas de los aplicativos, llevandolos a ser poco deseables para montajes masivos. Son inapropiados para montajes mixtos: por su misma concepción el montaje solicitado por las compañías cuenta con dos niveles de VPNs (la Intranet corporativa y luego las

Intranet de cada empresa), los cuales deben ser interrelacionados de manera armoniosa para flujo de información y control de acceso. Este tipo de montaje sería bastante costoso, difícil de implementar y de administrar con dos niveles de Firewalls.

7.5 Proxies un servidor Proxy, también conocido como un Gateway de aplicación, es realmente una aplicación ubicada para regular el tráfico entre dos segmentos de una red. Los Proxies son generalmente utilizados en lugar de los esquemas de filtrado para impedir el paso de la información entre dichos segmentos. El Proxy actúa como un intermediario y no permite la conexión directa entre los dos segmentos. Los Proxies no enrutan el tráfico, de hecho un Proxie bien configurado tienen las funciones de transporte desactivadas. Tal como su nombre lo indicas, el Proxy está ubicado entre los dos sistemas y establece comunicación entre ambos. Su funcionamiento podemos ejemplarizarlo. Un Host interno, quiere comunicarse con una pagina WEB que se encuentra ubicada en un servidor remoto, el host interno formula la requisición y la transmite al "Gateway" que en este caso es un Proxy, una vez que el Proxy recibe la información este determina que tipo de acceso se esta tratando de llevar a cabo, como en este caso el host ha requerido el acceso a una página WEB, el Proxy pasa la requisición a una aplicación especial usada sólo para procesar sesiones http. Esta aplicación es simplemente un programa que está corriendo en la memoria cuya única función es manejar los programas de comunicación con http. Cuando la aplicación recibe la requisición, revisa si ACL permite este tipo de tráfico, si el tráfico es permitido, el Proxy formula una nueva requisición al servidor remoto, cuyo ACL esta implícito en el Proxy, formula una nueva requisición y la remite al servidor remoto. Si viéramos esto a través de un analizador de datos, esto se vería como si el Proxy estuviera haciendo la requisición que originalmente se llevo a cabo desde el host interno, por esta razón cuando el servidor remoto contesta lo hace a el Proxy. Una vez que el Proxy recibe esta respuesta, nuevamente la pasa a la aplicación http donde es escudriñada para detectar si hay anormalidades en la información enviada por el servidor remoto, si la información es aceptada, crea un nuevo paquete y los pasa al host. Como puede observarse los dos extremos nunca se comunicaron entre sí y el Proxy constantemente se entromete en la conversación para asegurarse que todo esta funcionando como se espera. Los Proxy son utilizados para aplicaciones específicas, si se quiere soportar un nuevo protocolo en un Proxy, el Proxy debe soportar dicho protocolo

7.6 Virtual Private Networking (VPN) Desde que se introdujo la Internet ninguna otra tecnología había ofrecido tantas promesas como lo ha hecho VPN, o tal vez tantas controversias como VPN lo ha hecho, VPN se ha ofrecido como la cura para disminuir los gastos que supone WAN y al mismo tiempo como la solución del talón de Aquiles que supone la seguridad perimetral en ambiente de redes
Básicamente un VPN es un canal de comunicación sobre una red pública como Internet con autenticación y encriptación. Aunque la red continué siendo insegura la autenticación y la encriptación continúan protegiendo la data mientras esta en transito. Típicamente VPN es un servicio independiente, lo que significa que toda la información que se intercambia entre los Host intercomunicados se transmite a lo largo de este canal encriptado. Ello requiere una pequeña planificación antes de ubicarlos, las dos redes deben cumplir lo siguiente:

- ✓ Cada red debe tener un equipo capaz de servir como procesador VPN, puede ser un Router, un Firewall u otro equipo dedicado a cumplir actividades de VPN
- ✓ Cada ubicación debe conocer las direcciones de subred utilizadas por su contraparte
- ✓ Ambas ubicaciones deben aceptar un método de autenticación e intercambio de certificados digitales si es requerido
- ✓ Ambas ubicaciones deben acordar un solo método de encriptación e intercambios de claves de encriptación si esto es requerido

Una vez que el paquete original se encripta el Router encapsulará el texto cifrado (Ciphertext) en un nuevo paquete IP, usando su propia dirección IP así como la dirección IP del destino, este proceso es conocido como *Tunneling*, este proceso evita los ataques que tratan de husmear la información que se transmite entre los dos puntos conectados por VPN, pero lamentablemente no todos los sistemas VPN soportan este proceso. Con VPN se tiene adicionalmente el beneficio de tener un medio de transmisión seguro, no se requiere un software adicional de encriptación ya que todo ello sucede de una manera automática al pasar la información por los respectivos Routers lo que asegura que la información que anteriormente pasaba de

una manera "clara" puede ser transmitida sin ningún problema puesto que el proceso de encriptación no permite que la misma puede ser tomada.

VPN actualmente se viene utilizando como:

- ✓ Reemplazo de los MODEM de discado
- ✓ Reemplazo de links de WAN dedicados

Reemplazo de los MODEM de discado los MODEM de discado han constituido un problema para los administradores de redes, si bien son una solución estable, en muchos casos están muy por encima de los costos que una mediana empresa puede soportar. Una solución VPN para los usuarios remotos reduce los costos de soporte, ya no se requieren costos adicionales para soportar líneas de comunicación dedicadas, no se requiere hacer upgrade cada vez que un nuevo estándar de MODEM se hace presente o hacer upgrade a las líneas para soportar nuevas tecnologías tales como ISDN. Toda la información entrante es manejada vía Internet, una conexión que mantiene a su empresa haciendo negocios utilizando Internet

7.7 Gestión de Redes implica configurar, controlar y en algunos casos reconfigurar los componentes de la red con la finalidad de proporcionar prestaciones óptimas, tiempos de caídas mínimos, seguridad adecuada y flexibilidad. Para ello utilizamos un paquete de software diseñado para mejorar la gestión y fiabilidad de la red, la usamos fundamentalmente para identificar usuarios que representen un riesgo para la seguridad, identificar sistemas desconfigurados, detectar de manera proactivo problemas que se presentan en la red, mejorar las prestaciones de la red, hacer seguimiento del uso de los recursos y detectar tendencias que permitan pronosticar y tomar decisiones. El sistema de gestión de redes más común actualmente implementado es **Simple Network Management Protocol (SNMP)** para que esto suceda los equipos deben tener agentes SNMP. Los agentes y las estaciones de supervisión trabajan de manera conjunta a fin de dar al administrador de la red un punto central de control sobre los equipos de las redes.
La Gestión de Redes implica escuchar y monitorizar una red para que funcione como se planificó, las funciones que recomendamos sean llevadas a cabo en la institución comprenden:

- *Gestión de Fallos* se refiere a la detección, aislamiento y resolución de problemas de la red. Puesto que un fallo puede causar el mal funcionamiento de parte de la red o incluso de la totalidad de la red, la gestión de fallo proporciona un medio de conseguir que la red sea fiable. Así, la detección de un fallo en un enlace de la transmisión o en un componente de la red, la reconfiguración de la red durante el fallo para mantener el nivel de servicio y la restauración de la red cuando el fallo sea resuelto.
- *Gestión de Configuración* se refiere al proceso de configurar una red inicialmente y luego ajustarla como respuesta a los requisitos de cambios de la red. Esta función es quizás el área más importante de la gestión de redes ya que una configuración incorrecta puede ocasionar que la red funcione por debajo de lo normal o incluso no funcione
- *Gestión Contable* implica hacer el seguimiento del uso de los recursos de red, incluye monitorizar la carga de usuarios para determinar como situar mejor los recursos, de manera alternativa se puede examinar el tipo o nivel de tráfico que fluye a través de determinados puertos, administra igualmente las claves de red en coordinación con los Administradores Descentralizados de cada área
- *Gestión de Rendimiento* implica el control del uso de la red, del tiempo de respuesta de extremo a extremo y de otras medidas del rendimiento en varios puntos de la red. Los resultados del control se usaran para mejorar el funcionamiento de la red
- *Gestión de Seguridad* implica el cumplimiento de lo establecido en las políticas de seguridad en lo referente a control de acceso, autenticación, confidencialidad, integridad y no rechazo

Independientemente del producto que utilicemos para la gestión, una red contiene un cierto número de *dispositivos a gestionar* tales como bridges, Routers, servidores, estaciones de trabajo, etc. La gestión de redes implica controlar y/o alterar la configuración de estos dispositivos. Un *agente* que reside en el dispositivo gestionado, siendo sus tareas suministrar información de gestión acerca del dispositivo gestionado y aceptar instrucciones para configurar el dispositivo. Una *estación de gestión* que proporciona una imagen en forma de texto o gráfica de toda la red o uno de sus componentes, esta imagen es

proporcionada por una aplicación de gestión que reside en la estación. El intercambio de información entre el agente y el gestor se lleva a cabo usando un *protocolo de gestión de red*

Capítulo VIII

Virus

8.1 Generalidades uno de los problemas más frecuentes al que nos enfrentamos cuando hablamos de este tema es la indefinición, la gran cantidad de conceptos y lo poco preciso que son los mismos, nuestro primer problema al intentar abordar este capítulo es entender lo que es un virus y su diferencia con lo que realmente queremos abordar que son programas maliciosos. Probablemente la más sofisticada treta que pueda presentarse en un sistema computarizado es aquella que derrota las medidas de seguridad del computador y el que la institución ha establecido. La treta del virus no es más que la de un programa escrito para explotar estas vulnerabilidades. Podemos definir un virus en su fase más simple como un programa que tiene la capacidad de auto multiplicarse y distribuirse por diversos medios. Sus consecuencias sean "benigno o maligno" son las mismas, realiza una labor de multiplicación, de modificación de archivos que de manera habitual son archivos de programas, uniéndose a ellos y extendiéndose, de manera muy parecida a la actuación biológica de un virus que ataca y se expande a través de las células

8.2 Programas maliciosos existen dos tipos de elementos que podríamos clasificar dentro del ambiente de lo que constituye un programa malicioso, aquellos que requieren de un host para llevar a cabo su acción y los independientes de los cuales nos ocuparemos en este estudio y dentro de ellos especialmente los "virus" y los "worms". De acuerdo a su naturaleza pasa por uno de ls siguientes estados desde su inicio hasta su desaparición:

- *Fase Durmiente* está en reposo y eventualmente su estado es alterado por algún evento, como una fecha o la presencia de otro programa que lo activa, no todos pasan por este estrato
- *Fase de Propagación* en esta fase el programa coloca una fase estequiométrica de sí mismo en otro programa o en un área de un archivo, crea un clon e inicia su propagación
- *Disparo* comienza la ejecución de la misión para la cual fue programado, esta fase se activa por un elemento incidental
- *Ejecución* es la fase en la cual finalmente se ejecuta la acción programada

Muchos de estos programas trabajan de manera específica o son diseñados para un sistema operativo en particular, por eso al hacer este tipo de estudio debemos buscar paquetes antivirus que se aprovechen de las fortalezas del sistema y fortalezcan sus debilidades. Estos tipos de infección son perfectamente evitables si se conocen las causas que las originaron, pero lamentablemente este esquema no efectua. Por lo que debemos recomendar un programa educativo, que incluya un nivel básico de conocimientos acerca de la naturaleza de estos programas y sus riesgos.

8.3 Función del Antivirus la solución ideal para la treta de virus es prevención no permitir que los virus ataquen al sistema es el primer paso, pero sabemos que esto es dificil de lograr, pero aun con esto si logramos concienciar a los usuarios en cuanto al riesgo, lograremos reducir el número de ataques efectivos, pero si la prevención no funciona, los siguientes pasos que debemos considerar son:

- *Detección* una vez que la infección ha ocurrido trate de localizar el problema y su origen.
- *Identificación* posterior a la detección debe identificar el tipo de infección, eliminar el programa que lo ocasionó y evitar de esta manera su propagación.
- *Eliminación* deben eliminarse todas las trazas de la infección y restaurar el programa o archivo infectado a su versión original.

Muchas veces la identificación y eliminación se hace imposible en este caso la única solución que tendremos es *a partir de un respaldo reconstruir la versión original del archivo.*

8.4 Programas Antivirus podemos identificar cuatro generaciones de programas que han venido desarrollándose en una lucha constante entre los emisores de programas infectados y los programadores de las empresas que lucha para evitar la contaminación

- *Primera generación* es un rastreador del programa infeccioso que se basa en las características que estos programas tienen para ellos buscan un patrón lo que crea una "huella" que permite identificar la presencia de un virus. Dentro de esta primera generación también encontramos los

programas que conociendo la longitud que ocupa un programa en un archivo, actúan frente a cualquier variación

- *Segunda Generación* pasamos a la aplicación de reglas heurísticas, para detectar posibles ataques. En la mayoría de los casos se hacen búsquedas por fragmentos de código, que frecuentemente están relacionados con virus polimórficos, detecta la clave y descripta el virus para identificarlo y posteriormente erradicarlo. Este tipo de antivirus utiliza en algunos casos la suma de chequeo, puede alterar el programa pero no altera la extensión del mismo, proceso que utiliza para detectar la presencia de la infección
- *Tercera Generación* residen en memoria e identifican la infección por su acción, trabajan básicamente por sintomatología
- *Cuarta Generación* reúnen una gran cantidad de técnicas, entre ellas se incluyen actividades de rastreo y trampas activas, algunos de estos paquetes incluyen la capacidad de control de acceso, lo que limita altamente la capacidad de los virus de poder acceder a determinados archivos y por tanto la posibilidad de infección.

8.5 El Problema de los Virus en un estudio de PC Magazine[7], revela que cada incidente viral cuesta alrededor de $ 8100, en un trabajo que realice para la empresa PDVSA, llegue a la conclusión que una parada de un equipo independientemente de la causa suponía una pérdida de 258649.04$, para ello nos basamos en el sueldo promedio anual de un empleado que alcanzaba la suma de 39500$, lo que daba una rata de 18.99 por hora, una falla desde que se detectaba hasta que se solucionaba en promedio consumía 12 horas, lo que equivalía a 227.88$ el costo en productividad por equipo. Melissa afecto a 1135 equipos, lo que significa que por efectos de productividad de personal tendremos 258649.04$. Para el caso de la institución la situación es diferente ya que es muy difícil determinar las pérdidas pero podríamos establecer la siguiente premisa; en un estudio llevado a cabo por alumnos de la materia Seguridad Computacional se detectó que de 100 máquinas revisadas 67 tenían algún tipo de infección viral, no existe una política antivirus establecida, cuando se detecta un virus, la limpieza del equipo toma entre 3 a 4 días y se pierde en muchos casos la información que se almacenó. Si tomamos en cuenta que existe a la fecha alrededor de 12000 alumnos usuarios y en promedio usan el equipo 2 horas a la semana, y que cada alumno paga una cuota promedio mensual de 150 $, tendríamos que la negación de servicio por infección, seria para un estudiante de 0.86$ por hora, para un profesor o personal administrativo la cifra alcanzaría a 12.17$, pero en este medio la infección que presenta el estudio anterior nos mostró que para 25 máquinas sólo 6 presentaron este tipo de problemática y de ellas sólo 2 estaban fuera de servicio, en las otras cuatro se presentaban virus, pero lo desconocía el usuario. En la estimación de estos costos sólo tomamos en cuenta la negación del servicio, no evaluamos el tiempo perdido comprendido entre la estimación del servicio y la reanudación de la tarea, algunos estudios estiman que el tiempo de reanudación promedio es de 15 minutos[8]

8.6 Solución Propuesta a objeto de poder presentar una solución a la problemática que los virus presentan debe partir de dos elementos para la solución, uno sería la escogencia de algún software en el mercado que nos den la mejor relación costo / beneficio posible y en segundo lugar establecer una política que nos lleva a mitigar el riesgo que supone este tipo de software malicioso.
Para la primera solución pasamos a investigar y obtener una matriz que nos permitiera con los productos existentes en el mercado buscar la solución óptima para ello evaluamos los siguientes aspectos:

- Evaluación Tecnológica.
- Velocidad de Scanning.
- Ofrece Scan de Memoria.
- Ofrece Scan de Archivos entrantes.
- Ofrece Scan de sectores de boot.
- Ofrece Adiestramiento.
- Ofrece Apoyo en Instalación.

[7] Marzo 2000

[8] Weber Information Systems Control and Audit

- Actualización automática.
- Aviso de falla en actualización.
- Ofrece upgrade sin costo.
- Trabaja en todas las plataformas.
- Detecta Virus encriptados.
- Ofrece actualizaciones adicionales.
- Detecta Virus en Zip.
- Reporte de auditoria.
- Herramientas de desinstalación.
- Reportes de Scan.
- % de reparación en archivos dañados.
- Ofrece help desk 24x7x365.
- Actualización por la red.
- Detección y reparación de Macrovirus.

En las gráficas mostramos una tabla de evaluación realizada con los elementos de evaluación mostrados. Este estudio ha sido realizado en Enero del 2002, dado lo ajustado de los resultados, es conveniente hacer investigaciones independientes para sustentarlo, de igual manera es conveniente actualizarlo cada 6 meses si se quiere tomar alguna decisión, basándose en esta tabla de evaluación de tecnología. Al momento de realizar este estudio la organización Gartner, en su publicación de Enero coincide con el resultado que presentamos para el primero y segundo lugar.

8.7 Política Antivirus el objetivo perseguido por la política antivirus propuesta tiene como objetivo *seleccionar un producto y automatizar su operación a fin de implementar una política completa para contrarrestar la actividad viral y sus consecuencias a nivel de infraestructura de microcomputadores y redes*

8.7.1 Roles la política se sustenta sobre los siguientes componentes:

- *Administrador* se ubica en la organización de Infoseg, sus funciones básicas tienen que ver con la instalación, mantenimiento y distribución del producto seleccionado. Esta en contacto permanentemente con el escritorio de ayuda para dar soporte y en caso de no poder solucionar la problemática presentada, es la persona encargada de subir el caso al suplidor del producto y hacer seguimiento hasta lograr la solución definitiva a la problemática que se ha presentado
- *Analista Antivirus y de Laboratorio* trabaja conjuntamente con el administrador y lo suple en sus funciones cuando esta ausente, se encarga de aislar el virus, determinar como fue contagiada la máquina, mantener la cuarentena cuando sea necesaria, determinar el daño ocasionado con la infección y conjuntamente con el administrador diseñar medidas preventivas
- *Usuario/cliente* el usuario mantiene comunicación con el administrador y en caso de alerta informa al Escritorio de ayuda de la anomalía presentada

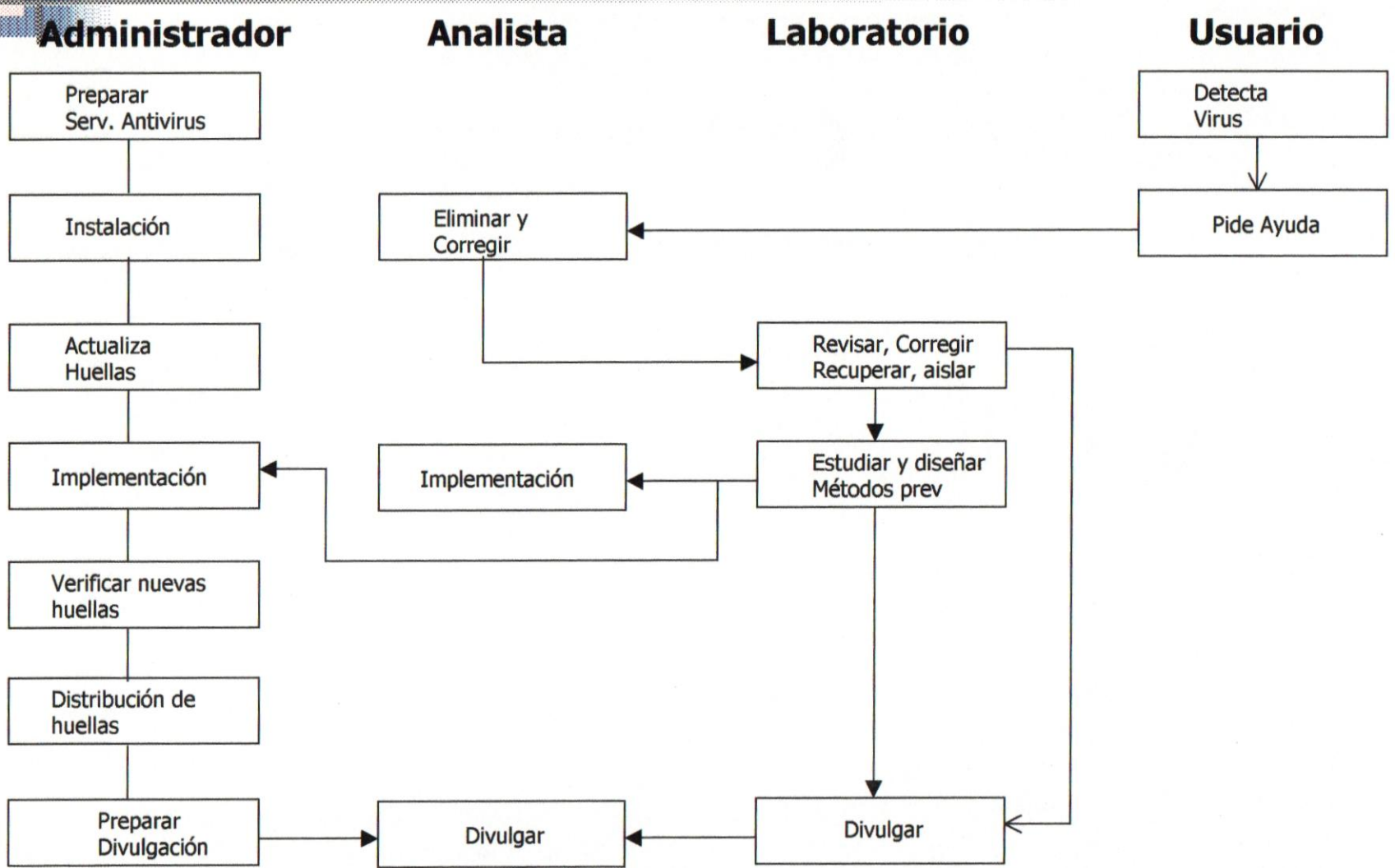
Ningún sistema de seguridad es 100% seguro. Por eso todo usuario de computadoras debería tratar de implementar estrategias de seguridad antivirus, no sólo para proteger su propia información sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados, por tanto debe instruirse al usuario y darle las herramientas necesarias a través del programa de inducción para evitar el contagio

Para implementar tales estrategias deberían tenerse a mano los siguientes elementos:

- ✓ **UN DISCO DE SISTEMA PROTEGIDO CONTRA ESCRITURA Y LIBRE DE VIRUS:** Un disco que contenga el sistema operativo ejecutable (es decir, que la máquina pueda ser arrancada desde este disco) con protección contra escritura y que contenga, por lo menos, los siguientes comandos: FORMAT, FDISK, MEM y CHKDSK (o SCANDISK en versiones recientes del MS-DOS).

- ✓ **UN PROGRAMA ANTIVIRUS ACTUALIZADO:** Se puede considerar actualizado a un antivirus que no de quince días desde su fecha de creación (o de actualización del archivo de strings).
- ✓ **UNA FUENTE DE INFORMACIÓN SOBRE VIRUS ESPECÍFICOS:** Es decir, algún programa, libro o archivo de texto que contenga la descripción, síntomas y características de los virus más comunes.
- ✓ **UN PROGRAMA DE RESPALDO DE ÁREAS CRÍTICAS:** Algún programa que obtenga respaldo (backup) de los sectores de arranque de los disquetes y sectores de arranque maestro (MBR, Master Boot Record) de los discos duros. Muchos programas antivirus incluyen funciones de este tipo.
- ✓ **LISTA DE LUGARES DÓNDE ACUDIR:** Una buena precaución es no esperar a necesitar ayuda para comenzar a buscar quién puede ofrecerla, sino ir elaborando una agenda de direcciones, teléfonos y direcciones electrónicas de las personas y lugares que puedan servirnos más adelante. Si se cuenta con un antivirus comercial o registrado, deberán tenerse siempre a mano los teléfonos de soporte técnico.
- ✓ **UN SISTEMA DE PROTECCIÓN RESIDENTE:** Muchos antivirus incluyen programas residentes que previenen (en cierta medida), la intrusión de virus y programas desconocidos a la computadora.
- ✓ **TENER RESPALDOS:** Se deben tener respaldados en disco los archivos de datos más importantes, además, se recomienda respaldar todos los archivos ejecutables. Para archivos muy importantes, es bueno tener un respaldo doble, por si uno de los discos de respaldo se daña. Los respaldos también pueden hacerse en cinta (tape backup), aunque para el usuario normal es preferible hacerlo en discos, por el costo que las unidades de cinta representan.
- ✓ **REVISAR TODOS LOS DISCOS NUEVOS ANTES DE UTILIZARLOS:** Cualquier disco que no haya sido previamente utilizado debe ser revisado, inclusive los programas originales (pocas veces sucede que se distribuyan discos de programas originales infectados, pero es factible) y los que se distribuyen junto con revistas de computación. Tratar en lo posible de evitar que el usuario pueda bajar información a su computador por una vía diferente a la establecida que es del Servidor de aplicaciones
- ✓ **REVISAR TODOS LOS DISCOS QUE SE HAYAN PRESTADO:** Cualquier disco que se haya prestado a algún amigo o compañero de trabajo, aún aquellos que sólo contengan archivos de datos, deben ser revisados antes de usarse nuevamente.
- ✓ **REVISAR TODOS LOS PROGRAMAS QUE SE OBTENGAN POR MÓDEM O REDES:** Una de las grandes vías de contagio la constituyen Internet y los BBS, sistemas en los cuales es común la transferencia de archivos, pero no siempre se sabe desde dónde se está recibiendo información.
- ✓ **REVISAR PERIÓDICAMENTE LA COMPUTADORA:** Se puede considerar que una buena frecuencia de análisis es, una vez a la semana

Solución Propuesta
Política antivirus



Capítulo IX

Sistemas Operativos

9.1 La integridad del Sistema Operativo los sistemas operativos son ante todo administradores de recursos; el principal recurso que administran es el hardware del computador: los procesadores, los medios de almacenamiento, los dispositivos de I/O y los datos. Los sistemas operativos realizan muchas funciones, como proporcionar el interfaz con el usuario, permitir que los usuarios compartan entre si el hardware y los datos, evitar que los usuarios se interfieran recíprocamente, planificar la distribución de los recursos entre los usuarios, facilitar la entrada y salida, recuperarse de los errores, contabilizar el uso de los recursos, facilitar las operaciones en paralelo, organizar los datos para lograr un acceso rápido y seguro y manejar las operaciones en la red. Como sea que se decida definir los sistemas operativos, lo importante es no olvidar que constituyen una parte integral del ambiente de cómputo, que los usuarios en muchos casos no lo comprenden y que desde el punto de vista de la seguridad es básico su comprensión y por ende su protección. En el año 1974 Stepczyk, identifico cinco elementos que deben mantenerse para que el sistema operativo mantenga su confiabilidad, estos aspectos hoy en día continúan teniendo plena vigencia, ellos son:

- *El sistema operativo debe ser protegido de los procesos de los usuarios.* No debe permitirse que un proceso de un usuario pueda sacar de servicio al servidor, que pueda destruir información esencial, tome control del sistema o cambie el sistema operativo sin autorización.
- *Los usuarios deben ser protegidos recíprocamente.* El sistema operativo debe prever que un usuario corrompa o altere los procesos y los datos del resto de los usuarios.
- *Los usuarios deben protegerse de las acciones que ellos mismos lleven a cabo.* Un usuario puede comprometer distintos módulos o subprocesos que tienen que ver con el área de memoria y los archivos que esta utilizando. Un módulo o subproceso no debería ser capaz de corromper otro módulo o subproceso.
- *El sistema operativo debe ser protegido de si mismo.* Al igual de lo que sucede a nivel de usuario, el sistema operativo deben autoprotegerse a objeto de que un módulo o subproceso pueda corromper otro módulo o subproceso.
- *Enfrentar satisfactoriamente los problemas ambientales.* Cuando se presentan problemas ambientales el sistema operativo debe ser lo suficientemente robusto para determinar las acciones a seguir al presentarse un problema ambiental

Las tretas que pudieran alterar la integridad del sistema operativo, pueden ser accidentales o deliberadas. Los problemas que pueden derivarse de *razones accidentales* incluyen fallas de hardware, software y sobre protectores de elementos ambientales, ellas pueden ocasionar fallas en los equipos, caídas de los sistemas operativos, o procesos con resultados inesperados. Las tretas de origen no accidental o *deliberadas* generalmente tienen como objetivo lograr el acceso a información o procedimientos para los cuales el usuario no esta autorizado, abrir brechas que les permita alterar la integridad de la data o la interrupción de las operaciones. Para lograr esto el que trata de llevar a cabo acciones deliberadas utiliza alguno de los siguientes elementos:

- Utilizar personal con privilegios y abusar de su poder
- Lograr utilizar los privilegios suplantando la identidad del usuario que los posee
- Utilizar equipos especiales que le permitan corromper la información
- Interactuar con el sistema operativo aprovechándose de una brecha descubierta

Entre los métodos más usuales que se utilizan para logra el objetivo perseguido podríamos mencionar los siguientes: Browsing, Masquerading, Piggybacking, Between-lines entry, Spoofing, Backdoors, Trapdoors, trojan horses. La integridad como hemos dicho proviene de fallas o debilidades que el propio sistema operativo presenta, entre ellas cabe mencionar

- *Parámetros incompletos de validación* el sistema no valida todos los atributos que el usuario ha exigido
- *Parámetros de validación incompletos* el usuario aplica esquemas de validación diferentes a los que recomienda el diseñador del sistema operativo, creando con ello debilidades

- *Compartimiento implícito de datos* en algunos casos se ubican datos sensitivos en áreas de uso común aspecto que facilita el compartimiento de los datos y por ende el no cumplimiento con lo que exige el usuario
- *Validación asíncrona* si el sistema operativo permite el procesamiento asíncrono de información, el usuario toma ventajas del parámetro de tiempo inadecuado para violar la integridad
- *Controles de accesos inadecuados* los sistemas operativos hacen una revisión incompleta o una parte del sistema asume que la otra ha desarrollado completa su tarea de revisión
- *Violación de límites impuestos* se decide imponer límites, pero el sistema no los valida y por ende son violados.

9.2 Sistemas Operativos básicamente la institución viene utilizando a nivel de servidores los sistemas operativos Windows NT, Linux y Unix. Por esa razón en el anexo 9, incluiremos algunas recomendaciones y sugerencias para la protección de dichos sistemas operativos

9.3 Monitoreo básicamente se utilizan dos tipos de monitores de software, el primero de ellos tiene que ver con los eventos que ocurren, al sistema operativo o a los programas, uno de ellos es el ***Accounting System*** que se encuentra incorporado en los sistemas operativos de multiusuario. Este monitor captura la consumición de recurso que ocurre y la data asociada con el usuario y el trabajo sometido que ocasiona esta consumición, un ejemplo de ello es un monitor simple que determina el comienzo y final de un programa, el tiempo de CPU consumido, las operaciones de I/O y la cantidad de memoria primaria y secundaria que se ha consumido. Este tipo de información básicamente se utiliza por razones de contabilidad y costos, pero también se utiliza con el objetivo de medir el rendimiento y la efectividad del sistema operativo. El segundo tipo de monitor que se utiliza es el ***Software Monitor*** que colecta información específica acerca de la efectividad de un determinado componente al darse una determinada señal en el tiempo.
Estos tipos de monitores deben ser observados a diario, deben establecerse parámetros de confiabilidad, determinar el cumplimiento de los convenios establecidos con los usuarios e investigar mal uso que se pudieran estar dando a los recursos así como tomar acciones que nos lleven al ajuste de los parámetros en el sistema operativo. Entre los elementos a los que debemos hacer este tipo de seguimiento podrían mencionarse los siguientes:

- El tiempo promedio que le toma a los usuarios acceder al sistema
- Cantidad de Usuarios rechazados por el sistema
- Accesos negados a archivos clasificados
- Actividad de los canales
- Caídas del sistema
- Tiempo de respuesta en horas pico
- Tiempo de negación de servicio por equipos, etc

Si bien estos esquemas son muy importantes para determinar la salud de nuestro sistema, su monitoreo nos lleva a tomar decisiones a posteriori, es por esa razón que hemos recomendado su utilización, con recursos que detecten la alarma, nos avisen y nos permitan tomar acción, aun antes de que un evento se de. Si bien en el mercado existen una serie de productos que cumplen con estas funciones, tales como: Tívoli, Hp Openview, InfoManagement, CA Unicenter, y otros. Cualquiera de ellos puede ser utilizado, la experiencia que tenemos nos permite recomendar el paquete de HP, sobre los anteriores, la razón para ello es que Openview esta muy orientado al monitoreo de redes, creo que la problemática que existe en la institución, esta muy relacionado con el establecimiento y cumplimiento con los Niveles de Servicio.

Capítulo 10

Recomendaciones

10.1 Seguridad Objetivo Estrategia y Metas a todo lo largo de esté trabajo, se ha establecido un esquema de protección específica, para una serie de problemas que presentan muchas de nuestras instituciones, que desde su inicio obviaron aspectos básicos de seguridad, y en su madurez requieren mecanismos específicos de protección. Pero el establecimiento de un esquema específico de seguridad, para solventar un problema, es actuar de manera reactiva y no siempre la solución aislada es el mejor beneficio. Basándonos en esta premisa es que hemos establecido un proyecto que tiene como objetivo final, dotar de mecanismos, a la institución a fin de aminorar la problemática de seguridad que es fácilmente detectable. En organizaciones grandes el establecimiento de un proyecto de esta índole no es una tarea sencilla, y su construcción no es inmediata, requiere una serie de pasos de riguroso cumplimiento, en cierta manera a lo largo de los capítulos que hemos presentado hemos mostrado esos pasos, pero es nuestro objetivo en este capítulo, establecer un engranaje que permita sin mayores sobresaltos establecer la organización de Seguridad y los mecanismos que la hagan eficiente.
La *lámina "Seguridad Objetivos Estrategias y Metas"*, que insertamos a continuación nos presenta un esquema resumido pero con una amplia visión de los pasos que debemos seguir que a nivel macro son los siguientes:

- Involucrar a las autoridades, haciéndoles entender que el problema de Seguridad de Información es de índole gerencial, pero tiene una solución tecnológica
- Educar a todos los usuarios, en sus diferentes estratos, acerca del valor de la información, que comprendan que la información es un *activo* y como uno de los activos más importantes de la organización requiere de una protección y una valoración que hasta ahora no se le ha dado.
- Establecer un grupo de trabajo, que teniendo el apoyo de las autoridades, establecerá las bases para la protección de los *activos de información*. Para ello seguirá un esquema tal como el que presentamos en la lámina referida

De esta primera fase surgirá un plan de trabajo que en principio hemos elaborado para los próximos tres años y que tiene como objetivos los siguientes elementos:

- Proteger la Información, de acuerdo con el valor que la institución ha establecido
- Establecer mecanismos de protección centralizada, para la información descentralizada
- Establecer mecanismos de auditabilidad y autenticación
- Lograr un mecanismo único y sólido de Control de acceso
- Establecer un esquema y los mecanismos que nos permitan obtener un administración centralizada
- Dotar a la institución de políticas y normas de Protección a los Activos de Información, así como de los mecanismos que aseguren su cumplimiento
- Crear la organización que administre la protección a los activos de información "INFOSEG"

El plan de trabajo que se ha diseñado, presenta tres *metas*, que deben cumplirse en el tiempo, para lograr el objetivo que nos hemos propuesto, estas tres metas a su vez las hemos distribuido en el tiempo de tal manera que:

- *En el primer año* nos avocaremos al establecimiento de las políticas y normas que nos lleven a obtener una base de sustentación para los mecanismos de protección de información que aplicaremos, esta fase estará reforzada con la divulgación y concientización del personal acerca del valor de los activos de información
- *En el segundo año* una vez establecida la base sobre la cual se construye la seguridad, viene la automatización de los mecanismos que aseguran su cumplimiento, de tal forma que buscaremos mecanismos que de manera proactiva nos alerten ante cualquier brecha y nos permitan mitigar los riesgos que hemos podido detectar en el paso anterior

- *En el tercer año* hemos completado la fase de automatización y debemos centrarnos en la continuidad y evolución del proyecto, para ello, tomaremos parte del personal que ha venido trabajando y con el formaremos INFOSEG.

Las *estrategias* las ubicamos en cuatro rubros, que al igual que las metas que nos establecimos verán su cumplimiento en el tiempo, ellas son:

- *Políticas y Normas* se inicia en el momento en que las autoridades aprueban y se involucran en el proyecto, se establecen las políticas y normas que sientan la base de protección a los activos de información y culmina con la creación de INFOSEG
- *Seguridad en Redes* su inicio, viene dado con el establecimiento de la arquitectura de tecnología, pasa por el análisis de riesgo, establece la arquitectura de seguridad, selecciona e instala los mecanismos que mejor se adaptan, a las políticas de protección de activos de información, que se han establecido. Todo ello sobre la base de un mecanismo de selección que del mejor valor al menor costo. Al final se integra a INFOSEG, como un grupo investigador de nuevas tecnologías
- *Control de Acceso* se inicia, con los mecanismos que permitan a la persona, al acceder a la información obtener sólo aquellas herramientas que requiere para cumplir con su labor, en un principio utilizaremos, mecanismos manuales, pero es el objetivo llegar a un mecanismo único e integral de Control de acceso
- *Seguridad Física* lo iniciamos con la revisión de las políticas de respaldo que se han establecido, y su concordancia con los elementos de riesgos encontrados y en concordancia con el valor de la información, pasa por el establecimiento de Planes de contingencia y culmina con el establecimiento de mecanismos de Control de Cambio y la corrección de las debilidades de seguridad física que hemos logrado detectar

10.2 Arquitectura de Seguridad partiendo del hecho de que hemos logrado levantar la información que nos permitió obtener el modelo de tecnología de la institución, nos toca ahora establecer el modelo de arquitectura de seguridad. Partamos de la definición [9]

- *Arquitectura "cualquier diseño o disposición ordenada percibida por el hombre".*
- *Diseño "Invención y disposición de las formas, partes o detalles de algo de acuerdo con un plan"*

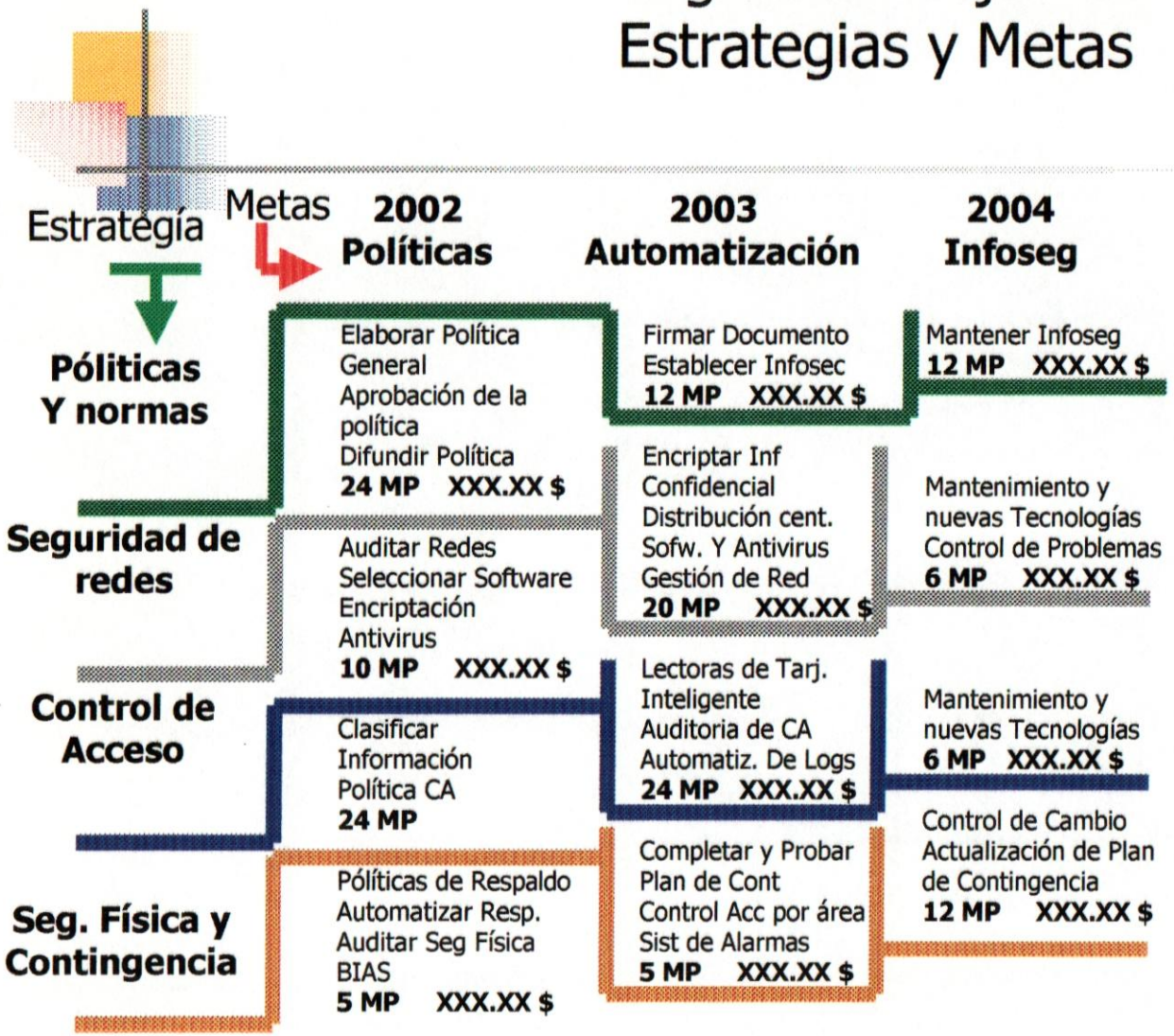
Tomando en cuenta esta definición establecimos el modelo de arquitectura de seguridad que podemos analizar en la figura *"Arquitectura de Seguridad"* anexa, la misma esta basada en el Estándar de Seguridad **ISO 11577.** Al tener la arquitectura de Tecnología, simplemente buscamos un estándar que cumpla con las características del modelo que hemos establecido, y de ahí en adelante, toda investigación tecnológica tendrá como base de sustentación el elemento anteriormente establecido.

El estándar *ISO 11577* especifica un protocolo para uso en sistemas intermedios y finales, que provee de servicios de seguridad a la capa de red (definido ISO 8348 e ISO 8648), que por tanto se convierte en el protocolo de seguridad de niveles de red (NSLP). Especifica:

1. Los siguientes servicios definidos en ISO 7498-2
    a. Autenticación de orígenes de datos
    b. Control de acceso
    c. Confidencialidad de la conexión y desconexión
    d. Integridad de la conexión y desconexión
    e. Prueba de origen
2. Los requisitos funcionales para la implementación que sigan este estándar, están definidos en términos de:
    a. Requisitos de las técnicas criptográficas que puedan usarse bajo este protocolo, tales como encriptación, prueba digital, control de acceso y notarización
    b. Requisitos de la información transportada, en asociación con la seguridad para la comunicación, tales como mecanismos de enrutamiento, autenticación e integridad

[9] The American Heritage Dictionary of the English Language

Seguridad Objetivos
Estrategias y Metas



Objetivos

- Proteger Información Crítica
- Seguridad Centralizada y descentralizada
- Auditabilidad Y Autenticación
- Acceso único
- Administración Centralizada
- Políticas y Normas
- Infoseg

10.3 Duración y Costos en el anexo *"Proyecto de Seguridad Cronograma"*, anexo, podemos establecer a nivel macro la duración del proyecto, para su completación se requieren aproximadamente 160 meses persona en un lapso de tres años, quedando finalmente como empleados fijos del INFOSEG, 3 personas que se encargaran de todo el manejo y mantenimiento de la organización.
El proyecto supone que en cada etapa se obtendrán una serie de productos que deben ser fijados conjuntamente entre la autoridad y el equipo desarrollador, estos productos, aparecen en el cronograma, que se establece y es la forma de medir la efectividad del proyecto, de igual manera supone la instauración de convenios de servicio y de reportes de efectividad, por medio de ellos se obtendran los avances y beneficios de este proyecto.
La función de costos es muy que depende de software y hardware adicional es muy difícil de establecer sin previamente haber completado el análisis de riesgo, pero en todo caso se trata de aprovechar al máximo las ventajas que da el sistema operativo en cuanto a seguridad, además aprovechar al máximo los paquetes que ofrecen seguridad a muy bajo costo, en todo caso podemos establecer algunos costos básicos, entre los cuales podríamos mencionar los siguientes:

Software	Costo	Instalación	Mantenimiento
Antivirus	45000.00 $	7000.00 $	6200.00$
Firewalls	9000.00		1200.00$
Single Signon	22430.00$	6000.00 $	3100.00 $
Seguridad de Red y Ws	42500.00 $		6500.00 $

Los costos se establecen en Dólares americanos, el mantenimiento se lleva a cabo mediante el pago de una cuota anual, los costos se han establecido sobre la base de 800 estaciones y 10 servidores. En estos costos no se incluyen equipos de monitoreo de red, que es básico para la centralización de la operación, la operaciones de líneas y seguimiento a problemas. En algunos productos el distribuidor requiere que se le paguen costos de instalación, los mismos suponen la venida de un técnico y los viáticos, por aproximadamente una semana

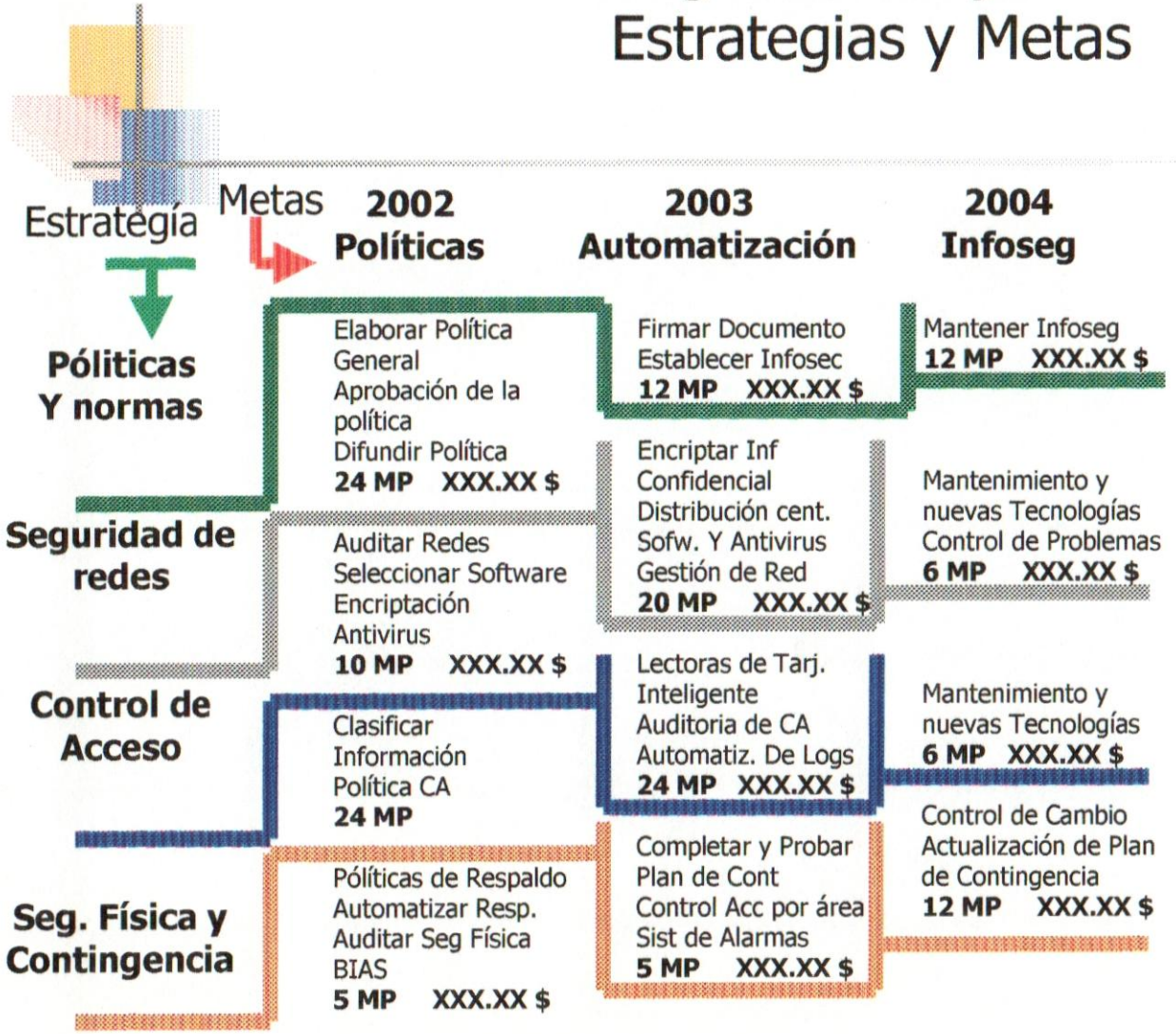
10.4 Los Retos del Siglo XXI si observamos las tendencias, podemos determinar que los retos a los que nos enfrentamos son fundamentalmente los siguientes:

- Incremento de la globalización, uso de Internet y todo tipo de conexiones que favorecen el negocio electrónico
- Incremento de tretas que tienen que ver con el espionaje electrónico
- Incremento de tretas que son llevadas a cabo por terroristas con grandes conocimientos de la tecnología
- Constante tretas contra la información veraz

10.5 Conclusión la seguridad, requiere una seria consideración por parte de las autoridades, todos debemos tomar en cuenta quienes y como nos están atacando y responder con las mejores armas disponibles y nunca tomar a la ligera el ataque que se nos pueda estar efectuando, debemos recordar que los ataques pueden provenir de cualquier punto del planeta, y que las instituciones gubernamentales y las instituciones de latos estudios, son un manjar muy apetecibles para los terroristas cibernéticos[10], la clave de la protección esta un esquema de seguridad que nos permita defendernos, pero con herramientas que nos permitan igualmente responder a los ataques. Debemos recordar que: *si bien es muy desagradable estar bajo una condición de ser atacado, lo es peor ser atacado y no saberlo o conocerlo cuando ya es demasiado tarde.*
A lo largo de este trabajo hemos revisado la importancia de la seguridad para la institución, la seguridad en forma general se ha tomado en cuenta al momento de presentarse un problema, pero no se ha manejado como un proyecto, esto ha traído como consecuencia que desaparecida la causa que origino el problema, nos olvidamos de la importancia que tiene trabajar bajo un esquema, de seguridad, que realmente tenga

[10] Gerald Kovacich, The Information System Security Officer´s Guide

Seguridad Objetivos
Estrategias y Metas



Objetivos

- Proteger Información Crítica
- Seguridad Centralizada y descentralizada
- Auditabilidad Y Autenticación
- Acceso único
- Administración Centralizada
- Políticas y Normas
- Infoseg

objetivos claros y que además, este investigando las nuevas tecnologías y sirviendo de apoyo a todas las organizaciones, que procesan la información y que cuando la requieren deben recibirla acorde con lo establecido en los convenios de servicio.

Este proyecto traerá los siguientes beneficios a la organización:

- Minimizará la pérdida de información valiosa
- Reducirá la cantidad de tiempo útil del cliente que se malgasta en la reparación de daños y problemas que presentan los equipos
- Aumentará la confianza del cliente en la infraestructura de micros y redes
- Se obtiene un cliente consciente y proactivo
- Agiliza el tiempo de respuesta de los organismos involucrados cuando se requieren soluciones

Si analizamos lo que hemos presentado a lo largo de este trabajo, podemos ver un objetivo muy claro que no esotro que: *Dar al usuario los recursos que requiere, en el momento que lo requiere para poder cumplir con su trabajo, acorde con las necesidades que la institución ha establecido*

Anexo 1
Políticas de Seguridad

I.-Introducción:

La información constituye uno de los activos de mayor valor para el cumplimiento de los objetivos de la institución, es por ello que a través de los procedimientos y políticas de manejo de la información, utilizaremos los mecanismos que apoyen su obtención, manejo y distribución de manera oportuna y relevante.

La tarea de proteger esta información se torna día a día más difícil y compleja motivado al incremento de la vulnerabilidad propiciada por una mayor accesibilidad a los canales de comunicación que nos permite la obtención de dicha información.

Para reducir el riesgo que implica el manejo de la información se requiere que todos los usuarios, posean conocimientos básicos sobre la terminología utilizada en el ámbito de Seguridad de Información y posea una visión de la función de protección de los activos de información dentro de la institución.

Es requisito básico para poder implantar estas políticas que la información clasificada este:

- Identificada y rotulada
- Su propietario identificado y que conozca sus responsabilidades respecto al manejo de la información bajo su responsabilidad
- El acceso a la información sea controlado
- Se elaboren planes de contingencia que permiten su recuperación en caso de desastre

II.- Normas para el Manejo de la Información Clasificada

A.- ¿Qué es la Información Clasificada? Aquella cuyo contenido debe tratarse con reserva por motivos pertinentes a la organización y que por tanto requiere un manejo especial con el objeto de impedir la divulgación de su contenido a personas no autorizadas para conocerlas.

B.- Control de Seguridad cada escuela designara una persona encargada del control de seguridad, quien administrará la recepción, custodia, registro, control y distribución de la información clasificada

C.- Alcance las normas que aquí se establecen serán de obligatoria aplicación, con el objeto de mantener la reserva deseada sobre toda la información de carácter clasificado, independientemente del medio en la cual dicha información este ubicada.

D.- Objeto de Estas Normas Aunque el intercambio de información es en si factor que contribuye a mayor entendimiento y comprensión y conduce a mayor facilidad y eficiencia para el logro de los objetivos de la institución. Existen ciertos documentos los cuales por la naturaleza de su contenido exigen un trato de reserva que variará según el documento. El objeto de esta normas es el establecer medidas prácticas para garantizar la reserva en el manejo por parte de los usuarios de la institución

E.- Responsabilidad por el Resguardo de la Información la eficacia de estas normas dependerá de la sincera cooperación y la discreción de los usuarios. Es por tanto sumamente importante que todo usuario conozca estas normas y comprenda cual es su responsabilidad en la protección de documentos clasificados. El registro y control de la información será responsabilidad de la ,máxima autoridad de la institución quien delegara en cada una de las escuelas esta responsabilidad en los directores quienes a su vez están encargados de nombrar un Administrador de la Información. El Departamento de Seguridad tiene la responsabilidad de suministrar ayuda y consejo sobre la estructuración de este procedimiento.

F.- Encargado del Control de Seguridad cada escuela, autorizará por escrito al personal seleccionado para el manejo de documentos

G.-Clasificaciones Usadas los términos "**Confidencial" y "Privado"** que a continuación se definen serán los únicos a usar dentro de la institución, con el fin de clasificar información de carácter reservado

CONFIDENCIAL el término CONFIDENCIAL, representa la máxima clasificación que usa la institución para la clasificación de documentos. Se usa para distinguir a la información para el conocimiento solamente de algunas personas, sobre la base de quienes necesitan la información. Se usará únicamente en aquella información que requiere protección porque su revelación puede incidir negativamente en los intereses o el prestigio de la institución

Privado es la clasificación usada como medio de seguridad para información oficial no destinada a circulación general. Este término se usa para distinguir los asuntos que se transmiten para el conocimiento del destinatario indicado y según lo determine esté último, también para otras personas autorizadas a quienes concierne la información y que la necesitan para la realización de sus labores. El termino PRIVADO será usado únicamente en aquella información relacionados con asuntos de la institución que por razones de reserva requieren cierto grado de protección en su manejo

III.- Políticas para el manejo de Información Clasificada en un Medio Electrónico

A.- Propósito la institución considera que la confidencialidad, integridad y disponibilidad de la información almacenada en sus centros y facilidades de computo son de vital importancia para el cumplimiento de su misión. En consecuencia tiene el deber y el derecho a proteger esta información mediante todos los medios que estén a su alcance. El presente documento establece la normativa de la Institución respecto a la protección y seguridad de la información y al uso de los recursos computacionales. Define la responsabilidad del usuario en el uso de las facilidades de computación, para tener una base sobre la cual tomar acciones en caso de que se efectúen violaciones a los puntos en él establecidos

B.- Roles

Computación es el encargado de suplir los servicios de procesamiento de datos y cumplir con las especificaciones de control de acceso establecido por el **Propietario**

Institución encargada de implantar las políticas, normas, procedimientos e instrumentos de control para garantizar el control, protección y confiabilidad de la información, según instrucciones del **Propietario**

Propietario es la organización en quien la institución delego la autoridad y responsabilidad para juzgar el valor, la importancia y el mantenimiento de la privacidad o confidencialidad de la información

Administrador Descentralizado es la persona en la que el **Propietario** delega la responsabilidad de administrar y autorizar el acceso a la información

Usuario toda persona autorizada a utilizar los recursos informáticos de la empresa, mediante un código o instrumento de acceso

C.- Responsabilidades

Administrador de Seguridad persona encargada de implantar las políticas, normas, procedimientos e instrumentos de control para garantizar la protección de la información de acuerdo a las instrucciones emanadas por el **Propietario.** Son sus deberes:

- ✓ Proteger la información acorde con lo especificado por el **Propietario**
- ✓ Divulgar las políticas, normas y procedimientos de control
- ✓ Implantar mecanismos de Control de seguridad para detectar infracciones a las normas de seguridad e informar al **Propietario**
- ✓ Instalar, mantener y actualizar los mecanismos de seguridad

Centro de Computación son sus atribuciones:

- ✓ Suplir los servicios de procesamiento de datos, cumplir con las especificaciones de acceso dadas por el **Propietario.**
- ✓ Diseñar e implantar procedimientos e instrumentos idóneos para garantizar la custodia física de la información y la conveniente utilización de los recursos computacionales de la institución
- ✓ Verificar la efectividad de los instrumentos de custodia de la información
- ✓ Tomar acciones efectivas y rápidas en caso de infracciones a las normas de seguridad
- ✓ Suministrar a el **Administrador de Seguridad y al Administrador Descentralizado,** los logs producidos por el sistema a fin de que puedan detectar anormalidades en los procesos

Escuelas o Departamentos

- ✓ Asegurar que la información que es entregada a Informática para su custodia sea válida y consistente
- ✓ Clasificar la información de acuerdo a lo especificado en el manual de **Normas para el manejo de la Información Clasificada** y autorizar su uso

- ✓ Velar por que los procedimientos de seguridad cumplan adecuadamente con su objetivo
- ✓ Informar a los niveles gerenciales y autoridades, por la vía máx. expedita posible acerca de las infracciones detectadas
- ✓ Designar a los **Administradores Descentralizados**

Usuarios

- ✓ Conocer y cumplir los lineamientos, las normas y los procedimientos sobre la protección y la seguridad de la información y el uso de los recursos computacionales
- ✓ Utilizar los recursos que le han sido confiados sólo para propósitos relacionados con las funciones que la institución le ha asignado
- ✓ Velar por que el uso de la información manejada se mantenga dentro de los medios y procedimientos establecidos a fin de garantizar la seguridad de dicha información
- ✓ Usar adecuadamente los recursos computacionales y comunicar cualquier anormalidad al **Administrador Descentralizado**

Administrador Descentralizado

- ✓ Divulgar y asegurar que se cumplen las normas, políticas y procedimientos de seguridad en su departamento
- ✓ Proporcionar a los usuarios la autorización para tener el acceso adecuado a los datos
- ✓ Detectar las infracciones a las normas de seguridad e informar al **Propietario** de la eventualidad
- ✓ Revisar los logs y utilizar las herramientas que suministra el **Centro de Computación** a fin de detectar violaciones que se pudieren estar cometiendo

Anexo 2
Análisis de Riesgo

1 Auditoria de Tecnología:

Tal vez nuestro primer problema al enfrentar un esquema de Análisis de Riesgo, sea el hecho real que supone el cambio drástico que esta teniendo la tecnología de la información, la obsolescencia de los equipos, lograr la mayor rentabilidad en las inversiones y finalmente poseer una plataforma tecnológica que cumpla con los estándares de desarrollo de la organización. De esta fase obtendremos un modelo que caracterice a la institución que objetivamente tratamos de definir

Desde el año 1960, los gastos en tecnología de información se han incrementado a una tasa interanual del 6%, con la excepción de 1985, en el que declina levemente, fenómeno que se explica por la aparición de los PC's, que crea ciertas confusiones en cuanto al rumbo que seguiría la tecnología. Al mismo tiempo los costos de hardware, comunicaciones y software han declinado rápidamente lo que nos ha permitido introducir gran cantidad de tecnología, que a su vez ha traído como consecuencia la pérdida de gran parte del control y en muchos casos la gerencia esta altamente preocupada por saber como integrar esta montaña de tecnología que se ha introducido en los últimos diez años y para ello requiere conocer de la realidad de su empresa mediante un proceso de **Auditoria de Tecnología de Información.**

El proceso de auditar **Tecnología de la Información** esta basado en una metodología que paso a paso nos permitirá analizar casi de manera particular la situación de una institución, por tanto es un proceso altamente particular. El proceso comienza por recolectar la información acerca de la organización, los objetivos de la institución y las operaciones del día a día. Esto nos ayudará a entender como y por que se han implantado sistemas específicos, a identificar áreas o tareas que pueden ser más eficientes o a realizar modificaciones en los sistemas o implementar nuevas tecnologías.

En los últimos años al mismo tiempo que las compañías enfrentan el impacto de las redes globales, las gerencias han comenzado ha cambiar de parámetros de competitividad a parámetros de supervivencia, el pensamiento de la gerencia esta basado de manera primaria e intuitiva en invertir en el despliegue de tecnologías que catapulten a su empresa y pueda tomar las ventajas que Internet supone, en vez de tratar de ahorrar en su inversión o prever las ganancias que obtendrá basado en su inversión. Esta mentalidad de supervivencia nos permite explicar porque se están invirtiendo grandes sumas de dinero en el desarrollo de Internet Sites, aunque no se espera obtener provecho de ello en al menos tres o cinco años.

Aunque en principio alinear las estrategias de IT con las estrategias del institución a fin de lograr ventajas competitivas es un objetivo razonablemente positivo, en la práctica es muy difícil de lograr. La principal razón viene dada en que un gerente de IT debe balancear los objetivos a corto plazo de la institución y proporcionar un servicio confiable, con las estrategias de largo plazo que le permitan mejorar su competitividad y asegurar que la organización sobrevivirá al impacto de la tecnologías emergentes.

Este proceso de alinear estrategias de IT con los objetivos de lal institución ha pasado por cuatro diferentes fases:

- ✓ **1970's Sistemas Funcionales**
  - IT automatizando funciones en cada departamento
  - Prioridad en implementar sistemas funcionales
  - Arquitectura centralizada y procesos en batch
- ✓ **1980's Sistemas Interoperables**
  - Sistemas compartidos por múltiples departamentos, se automatizan funciones específicas y se comparte información.
  - Prioridad en automatizar la empresa
  - Arquitectura descentralizada, bases de datos relacionales
- ✓ **1990's (primera parte) Reingeniería**
  - Sistemas a todo lo largo y ancho de la empresa, se utilizan para lograr la reingeniería de áreas específicas del institución a fin de mejorar la competitividad

- Prioridad mejorar la competitividad y mantener los costos
- Arquitectura de redes, computación interactiva

✓ **Hoy Sistemas de nueva generación**

- Los sistemas permiten explotar oportunidades de instituciones resultantes de innovaciones tecnológicas, Network Computing System produce una reevaluación de los procesos del institución
- Prioridad sobrevivir el impacto que las nuevas tecnologías traen al modelo fundamental del institución
- Arquitectura Network Computing, soporte de estándares de Internet

1.1 Estrategias de IT

Definitivamente es muy difícil integrar un mapa de estrategias de IT con los objetivos de la institución, estrategias específicas de IT como la implantación de Fast Ethernet, o un backbone ATM, o la implantación de Lotus Notes o Microsoft son difíciles de interconectar con los objetivos estratégicos del negocio. Estos elementos de IT son justificados a través de sus ventajas tales como "mejorar el trabajo del individuo, o la habilidad para trabajar en grupo, o mejorar la calidad y el tiempo de las decisiones gerenciales ", la realidad nos indica que los sistemas de información son en extremo complejos y en muchos casos son diseñados para soportar requerimientos específicos.
Pero a pesar de lo dicho anteriormente creemos que alinear las estrategias de IT con las de la institución, es un reto y el mismo puede lograrse si se entienden los objetivos de su institución, los objetivos de sus sistemas y al mismo tiempo conoce las tecnologías emergentes.
El proceso de auditoria de tecnología de información es diseñado a fin de lograr su comprensión y a la vez lograr dos objetivos básicos; mantener la efectividad de costos de sus aplicaciones críticas y buscar la actualización o reposición de las mismas a fin de mantener la efectividad y competitividad y sobrevivir al impacto de las tecnologías emergentes comprendiendo al mismo tiempo como lo impactaran a Ud. y al modelo de su institución.

Objetivo del Negocio:

Los gerentes de IT se enfrentan a una constelación de presiones a fin de conocer el objetivo de su institución:

- Demanda de los usuarios a fin de que se les proporcionen servicios adicionales, mejorar la eficiencia e incrementar la efectividad todo ello sin incrementar los costos
- La competitividad lo obliga a buscar nuevas tecnologías
- Competitividad interna, los consultores internos, los suplidores externos y el mismo conocimiento del personal, hacen complicado los incrementos de costos, ya el departamento de IT no es el único proveedor ni tiene el monopolio de la información
- Los gerentes de la institución se vuelven conscientes del valor que una compañía de información puede tener y que esto puede eclipsar el valor de sus productos y servicios.

Para disminuir el efecto de estos elementos IT debe hacer reingeniería sobre cualquier práctica, procedimiento o actitud que pueden convertirla en obsoleta o irrelevante:

- **Actitudes Obsoletas** El hecho de tratar de convertir al usuario en un "Conocedor amplio del área; Internet y otros elementos" no se requieren amplios conocimientos para manejar la información.
- **Prácticas Obsoletas** Invertir en tecnología obsoleta a fin de ahorrar costos
- **Procedimientos obsoletos** Creer que IT suplirá toda la información cuando la tecnología permite sin mayor esfuerzo al usuario obtener la información que requiere

1.2 Gerenciando Tecnología de Información El proceso de Auditoria de Tecnología de la Información es una metodología que debe seguirse paso a paso y que le permitirá analizar la situación única de su institución. El proceso comienza reuniendo información acerca de sus objetivos, su organización y las operaciones del día a día. Esto le permitirá comprender el porque de la instalación de ciertos sistemas, determinará tareas que pueden manejarse de manera más eficiente bien sea subiendo el nivel ciertos sistemas o cambiando de tecnología.

En este proceso se evaluarán los siguientes aspectos de su organización:

- Misión
- Objetivos
- Operaciones rutinarias
- Tecnología de Sistema de Información
- Departamento de Sistemas
- Desarrollo y soporte In House
- Seguridad y disponibilidad de la Información
- Planificación de Tecnología de Información

La primera prioridad para un auditor es comprender los objetivos del cliente, que lo ha llevado a requerir una auditoria y a su vez reconciliar cualquier diferencia entre las expectativas del cliente y los servicios que proporciona. El siguiente paso será tratar de aprender tanto como le sea posible acerca de los factores que el cliente cree que son responsables para el éxito del negocio. En el proceso de reunir la información, el auditor logrará comprender como opera la institución y tendrá la oportunidad de establecer una estrecha relación de trabajo con el grupo gerencial

1.3 El Impacto de las Tecnologías Emergentes Es muy difícil identificar un segmento de nuestra economía que no haya sido impactado por tecnologías emergentes de telecomunicaciones o de computación. Virtualmente en el exitoso provecho y competitividad, esta la presencia de una decisión tecnológica a tiempo que mejora el rendimiento y la ventaja. Identificar las tecnologías que pueden reducir sus gastos en las operaciones y mejorar la competitividad de su institución son los elementos que debe mantener en mente al analizar el impacto que las nuevas tecnologías tendrán sobre la base neural de la institución

1.3.1 Data Storage El costo de almacenamiento de la información esta declinando rápidamente, tanto la memoria de corto plazo como la de largo plazo están pasando por circunstancias similares que la de los procesadores, se están convirtiendo en más poderosas, más pequeñas y de menor costo. Un ejemplo de ello podría ser el DVD, que almacena mucha mayor cantidad de información, a un menor costo y mayor velocidad de procesamiento, siendo capaz de almacenar 7 GB, capaz de almacenar 2,5 horas de vídeo y con óptima calidad de sonido todo ello en un disco estándar

1.3.2 Periféricos Aunque a menor escala los periféricos también presentan sustanciales reducciones, una impresora que en 1986 costaba alrededor de 5000$, cuesta hoy menos de $ 500

1.3.3 Otro Software El movimiento del software también esta presentando cambios a ritmo vertiginoso, las aplicaciones de software están mejorando la interoperatividad, la funcionalidad y la facilidad de compartimiento de datos, de igual manera es notorio la facilidad de uso.

1.4 Tecnologías Emergentes Existen muchas tecnologías que cooperan con la institución a fin de reducir costos, obtener mayor provecho y desarrollar nuevas oportunidades de institución.

1.4.1 1980 la revolución del PC permitió automatizar muchas funciones tediosas de oficina, tales como la creación y edición de documentos, permitió la descentralización de la información. Lo primero que se experimento detrás de esta revolución, fue que los usuarios tenían mejor acceso y control de la información que requerían para lograr los objetivos de su institución. Se desprende de esta revolución, una segunda situación de máxima importancia y fue que el usuario se independizo del personal de IT quienes de alguna manera les limitaban el acceso a la información crítica de la empresa y por tanto el proceso de toma de decisiones se agiliza y se mueve del headquarters a las oficinas regionales, los sistemas se propagan en la organización, el mainframe, pasa a ser grandes servidores en el proceso de distribución de la información y los PC's inteligentes pasan a ocupar el lugar de los terminales y más de 140 millones de PC's han pasado a ocupar el lugar de los terminales.

1.4.2 1985 las Redes La revolución del PC, fue eclipsada por las redes LAN, compuestas por PC's y una serie de recursos que podían ser compartidos, tales como impresoras, unidades de almacenamiento, etc., esto permitió continuar expandiendo su inversión en tecnología de PC's. Los usuarios logran a su vez un

más fácil acceso a las bases de datos corporativos, compartir información y utilizar el correo electrónico. Pero esto a su vez trajo consigo toda una serie de problemas, que en muchos casos aun no están resueltos tales como la seguridad, la integridad de la información y todos los problemas operativos que desde entonces han plagado el ambiente de IT.

1.4.3 1990 El cliente, el servidor y el no conectado. En los años 90, la industria comienza a moverse al modelo cliente-servidor. Esto permitía tener aplicaciones que compartían tareas entre aplicaciones "cliente" las cuales corrían en los PC's de la red y servidores en los cuales corría una poderosa base de datos, además de contar con servidores de comunicación, desde el punto de vista del hardware aparece el concepto de 'cluster" que permitía interconectar varios procesadores y de esta manera disminuía la probabilidad de fallas, proporcionaba igualmente escalabilidad y alta disponibilidad, para el usuario este esquema aparecida como un sólo computador en vez de un cluster con múltiples sistemas. Esta solución evolucionó hasta permitir el acceso remoto utilizando elementos digitales de alta velocidad e integradores "POP" (Point of Presence) nos proporciona una solución integrada por servidores remotos, Routers y firewalls.

1.4.4 1995 La recentralización_ Es en este año cuando los gerentes de IT, comienzan a entender la manera de implementar y operar aplicaciones cliente servidor, lo que trajo un cambio de paradigma que trae como consecuencia la aplicación del Network Computing Architecture que no es más que la reingeniería de cliente servidor, y comienza a denominarlos componentes de software basados en objetos distribuidos. Esta estructura pudiera haber muerto al nacer, pero ella proveía una solución con estructuras más robustas y eficiente que las redes LAN. Pero esta estructura nos vuelve al esquema de centralización, nos da clientes relativamente débiles con servidores de gran poder **Network Computing:** Permite a los usuarios de una manera transparente, acceder programas, datos o cualquier tipo de información desde su propia estación de trabajo, sobre su red LAN y/o en la Internet, estando el servidor ubicado en cualquier lugar, lo que nos presenta el siguiente esquema:
La Internet usa protocolos estándares basados en HTTP (Hyper Text Transfer Protocol) y le permite al usuario acceder información que esta almacenada en diversos servidores que son identificados por el URL (Universal Resource Locator).
Además Internet utiliza un formato estándar de documento HTML (Hyper Text Markup Language) para publicar la información en las páginas WEB y un browser WWW puede leer cualquier página almacenada en formato HTML.

1.4.5 Convergencia_ Dentro de 3 años, será posible comprarse un equipo que probablemente tendrá las dimensiones de un cellular, con suficiente ancho de banda el cual nos proveera integrar la voz, acceso a internet, entretenimiento y funciones de asistente personal[1], hoy lo vemos en los nuevos modelos de Palm

1.4.6 Internet_El uso primario de Internet hoy es el de mensajes electrónicos, pero actualmente muchas compañias lo están utilizando para dar soporte o vender sus productos. Los institucións a si como los departamentos y facultades la utilizan ya que sus productos y servicios pueden ser digitalizados y comunicarse con ellos electrónicamente han sufrido un fuerte impacto en su modelo, pero eventualmente cada distribuidor, detallista, manufacturero y/o organizaciones de servicio agregan valor al crear y distribuir ideas que serán impactadas por la convergencia entre computadores, comunicación y media. En el ambiente Universitario, la educación a distancia pasa a ser un elemento clave para el ingreso de nuevos alumnos a la institución, por otro lado Internet se vuelve un elemento básico para la comunicación y democratización de la educación
Entre las aplicaciones actualmente existentes en Internet cabe mencionar:

- Correo Electrónico
- Listas de distribución
- Transferencia de archivos(FTP)
- Electronic Bulletin boards
- Chat
- Comunicación de voz
- Videoconferencia
- Compra y ventas digitales

[1] Gartner Group, Conferencia Otoño Orlando Florida, 1999

- Servicios de soporte al cliente
- EDI

1.5 Hoja de Trabajo de Auditoria La primera fase de una auditoria de tecnología de información es completar la auditoria estratégica de la institución y esta incluye un grupo de hojas de trabajo detalladas que ayuden a definir y comprender el objetivo de la institución, la posición de sus productos en el mercado y analizar la operación de su institución. Esta fase también permite evaluar que áreas de su institución requieren de reingeniería a fin de alinear sus sistemas de información con sus objetivos incrementando los beneficios, disminuyendo gastos e incrementando oportunidades. De igual manera se deben contemplar las áreas de la institución que pudieran beneficiarse de tecnologías emergentes. Finalmente esta fase de la auditoria puede servir para cumplir con una serie de objetivos

- Identificar áreas que requieren reingeniería para mejorar la productividad, disminuir gastos, mejorar la productividad y permitir ingreso a nuevos mercados
- Ayudar a preparar un plan de institución
- Revaluar el modelo del institución
- Evaluar oportunidades de asociaciones o adquisiciones

Dentro de los objetivos de la auditoria cabe mencionar los siguientes

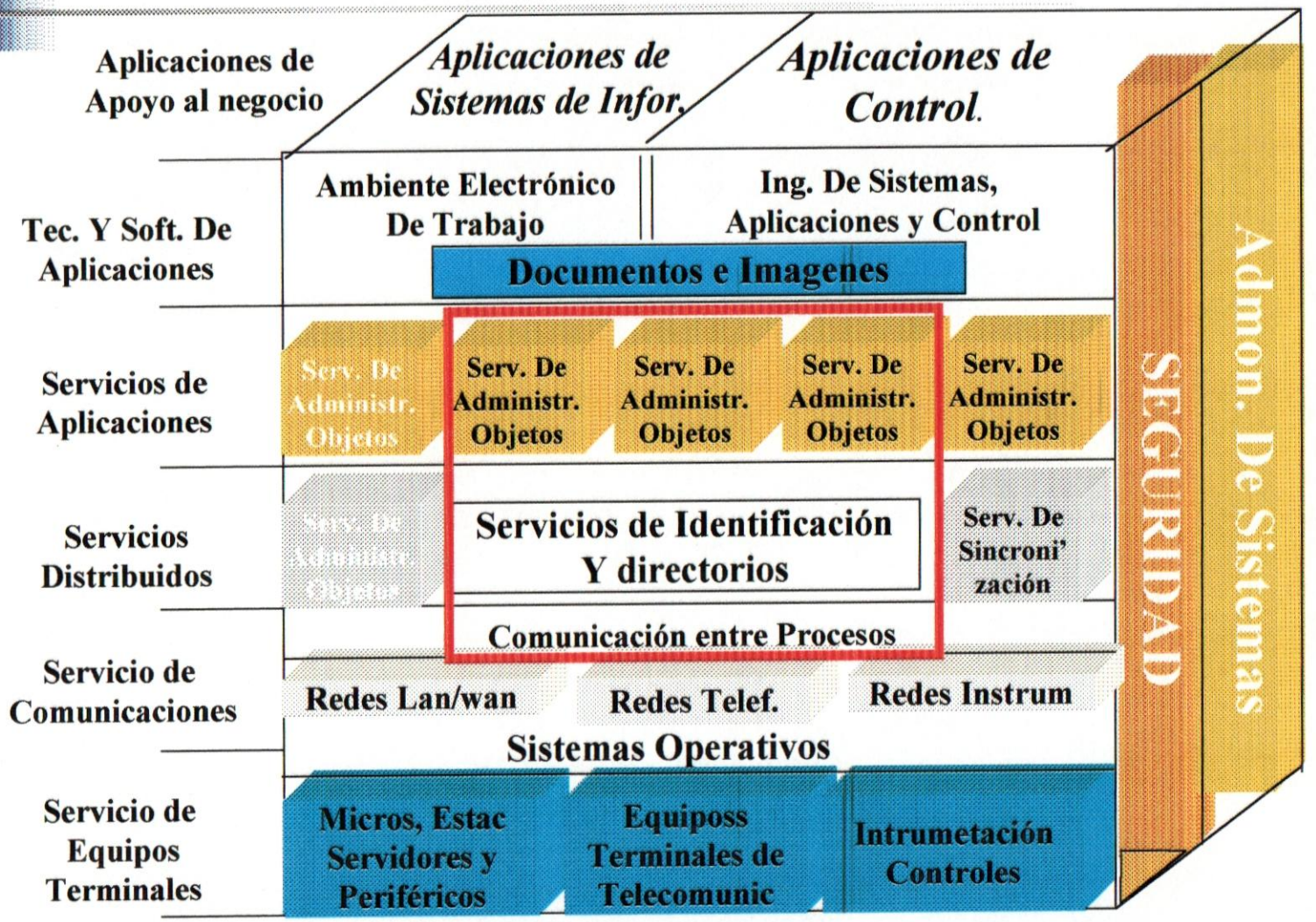
- Evaluar la infraestructura de IT a fin de determinar si es o no consistente con los objetivos del institución.
- Evaluar si el institución esta en línea con otras instituciones similares y determinar si podemos reducir los costos sin necesidad de desmejorar los niveles de servicio.
- Evaluar si es ventajoso o no el outsourcing
- Evaluar las habilidades de nuestro personal
- Evaluar el impacto que Internet tiene en el modelo de nuestro negocio. Evaluar la factibilidad de usar Internet para apoyar a nuestro mercado, servicios y clientes.

Como resultado de esta primera fase obtendremos básicamente un modelo del negocio tal como el que presentamos en el ***"Anexo 2 Figura 1"***, si este modelo lo alineamos con los estándares y productos de la institución, lo actualizamos en el tiempo, hacemos que entre capa y capa del modelo haya puntos de convergencia, tendremos un modelo dinámico, que nos permitirá cumplir con las exigencias de la Auditoria de Tecnología, que hemos analizado en estas páginas.

El modelo que presentamos a continuación funciona de manera similar al modelo OSI, vamos desde la capa más simple que es la que nos permite agrupar el hardware que utilizamos, pasamos por los sistemas operativos, revisamos los estándares y utilities de las organizaciones que nos permitan unificar el software de acuerdo con las conveniencias de la institución y finalmente sobre ella ubicamos las aplicaciones que el modelo tendrá que soportar.

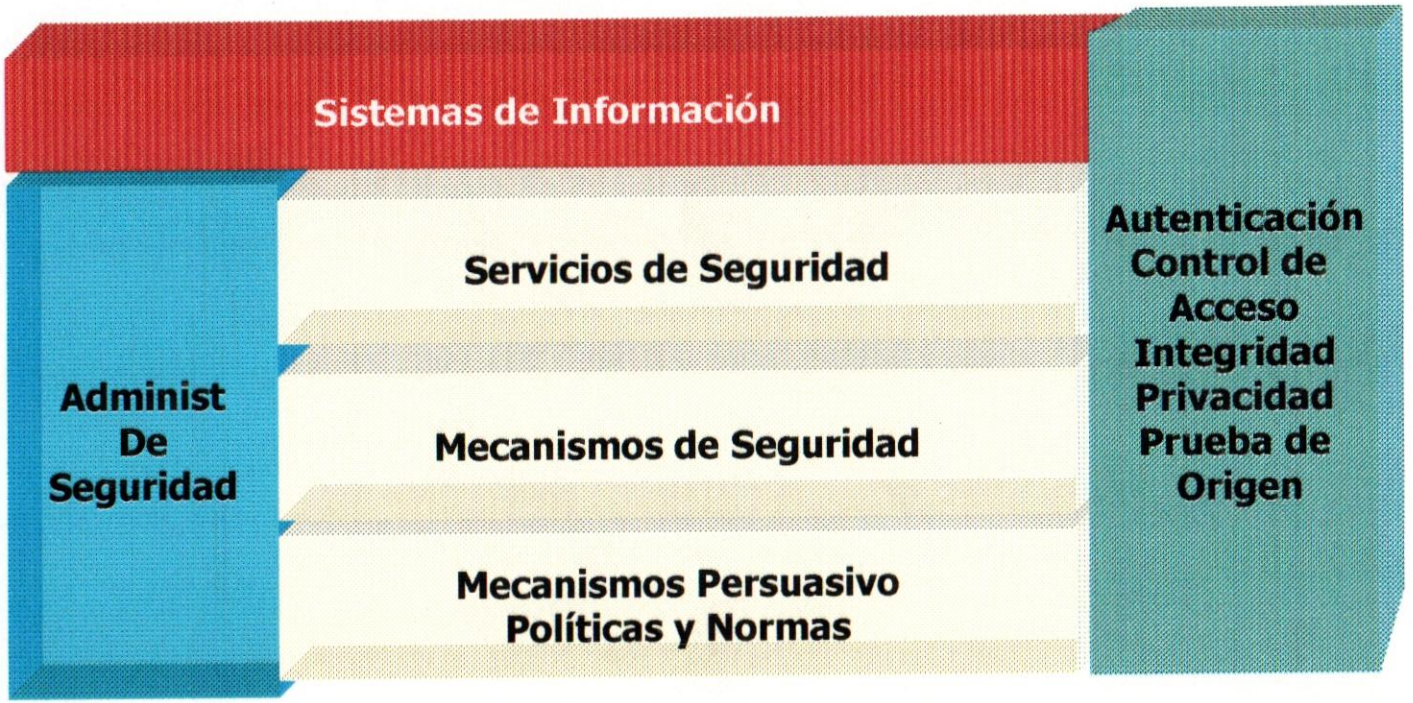
Este modelo a su vez funciona con los estándares de la ISO, de tal manera que al requerir un nuevo producto, analizo a que capa del modelo presentado corresponde, determino que estándares ISO utilizo en dicha capa, y que elementos de convergencia tiene con las capas superiores, realizado este análisis es muy simple escoger el producto ya que el mismo debe cumplir con los estándares establecidos como fase inicial al momento de adquisición, de no cumplir con la especificación simplemente el producto se desecha.

Arquitectura de Sistemas



Arquitectura de Seguridad

Arquitectura de Seguridad Standard ISO 11577



2 Auditando la Red

La red es el tendón de Aquiles de las empresas modernas, si la red puede ser penetrada estamos dando al Hacker una trinchera, en alguno de los servidores que conforman la red, desde ese punto puede determinar un plano de la red y con dicha información atacar las distintas plataformas presentes en la red. El que no realiza actividades de Hacker en su propia red no puede tener idea acerca de la seguridad de la misma, por tanto pareciera ser un requisito para lograr la seguridad el determinar la capacidad de defensa que la misma tiene frente ataques simulados, al logra un punto de falla debemos explotarlo, documentarlo y finalmente buscar la herramienta que nos permita reducir el riesgo.
Como profesionales de seguridad debemos estar conscientes del riesgo que representan conexiones no autorizadas a la red, de la data no protegida, de los virus, los esquemas de autenticación y control, igualmente es nuestro deber conocer los problemas que estas debilidades causan en la red y la magnitud de hasta donde pudieran llegar estos daños.

2.1 El Carrier en la medida que la información se convierte en interactiva, el proceso permea a las organizaciones de la institución, por tanto se hace necesario identificar los procesos críticos, una vez identificados deben establecerse medidas que permitan redundancia donde la misma sea requerida a fin de hacer que esos procesos se conviertan en procesos tolerantes a fallas, en las grandes empresas que se desarrollaron a través de un mainframe en un ambiente centralizado, a los sitios críticos se les establecía un ambiente de comunicación redundante, si los costos lo permiten y el tipo de transacción crítica que manejamos lo requiere este es un buen método, pero antes de tomar la decisión requerimos analizar las transacciones ya que muchas de ellas no son dependientes del tiempo lo que nos da soluciones alternativas, como es almacenar la transacción y al momento en que el tráfico disminuya enviarla, manejando esta información en un ambiente que podríamos definir como "near line", con ello reducimos las cargas y podemos determinar realmente el ancho de banda requerido al momento de una emergencia. Este método supone que demos prioridad a las transacciones críticas. Estas transacciones críticas deben tener *múltiples opciones de conectividad* a fin de poder re enrutar la transacción al momento de presentarse algún problema en el camino. Cada organización dentro de la institución debe ser analizada para identificar los procesos críticos, las transacciones a su vez deben ser prioritizadas tomando en cuenta por supuesto la opinión del dueño de la información quien es realmente el que conoce la necesidad de dicha información y su importancia relativa para el negocio. La transacción por último debe tener una medida relativa que denote su importancia, medida que ira de 0 para ninguna importancia a 10 máxima prioridad.
Una vez obtenida dicha información debemos armar una tabla en la que aparecerán por unidad del negocio y por tipo de transacción la siguiente información

Unidad del Negocio xxxxxx Función xxxxxxx Persona Contacto xxxxxxxx

Proceso	Transacción	Criticidad	Circuito	Dirección	Circuito Alterno	Dirección
Inscripción	Matricula	8	CD153645	142.114.24.02	no	
	Notas	10	CD153645	142.114.24.02	CD154654	142.115.16.01

Con esta información podemos proceder a la determinación de cuanta redundancia requeriremos y pasaremos a un proceso conocido como "Multipathing", que nos indica que una transacción puede en caso de falla tomar un diferente camino, es muy importante tomar en cuenta que el hecho de tener un diferente carrier no garantiza el Multipathing ya que en algún punto de la red pudiera estar utilizando la misma conexión, es por ello que las instituciones centralizadas como la Universidad que tienen su sede y una serie de sedes adicionales, pero que requieren la información de la sede central, deben considerar ciertas alternativas tales como conexiones satelitales que reduce la dependencia que tenemos sobre el carrier local.
El proceso en si consiste en establecer un contrato con un segundo carrier, usando rutas diferentes o facilidades alternas para ello (Frame Relay, Microondas o satélites) como alternativas, una vez completado esto establecemos los circuitos adicionales para cubrir las transacciones críticas, debemos una vez

completado este proceso además de documentarlo e incluirlo en el Plan de Contingencia, probarlo a fin de asegurarnos que la redundancia que hemos establecido, funciona de manera apropiada

2.1.1 Programa de Auditoria para el Carrier el programa de auditoria se dirigirá a determinar los siguientes aspectos:

- Determinar el tipo de carrier y los servicios que usa la institución
- Revisión del contrato que se ha establecido
- Revisar la documentación que llevo a la selección del carrier
- Revisar los costos y los servicios que el carrier ofrece, justificar el uso de cada uno de los servicios contratados.
- Revisar los procedimientos de monitorear la efectividad y cumplimiento del carrier
- Documentar y analizar los procedimientos para monitorear los servicios que ofrece
- Determinación de los servicios sobre/sub utilizados
- Establecer procedimientos que permitan medir a nivel de carrier:
  - MTBF(tiempo medio entre falla)
  - Niveles de Servicio
  - Mantenimiento y tiempo de respuesta

Tomando en cuenta los objetivos anteriormente señalados procederemos a establecer los elementos de riesgo asociados construyendo para ello una matriz de riesgo y control a manera de ejemplo presentamos la siguiente:

Matriz de Riesgo para Carriers

Riesgo	Control
La información que enviamos se puede corromper o perderse al utilizar como medio de transmisión Frame Relay o ATM si no utilizamos otros controles a nivel de aplicación	Establecer rutinas y técnicas de balanceo que nos permita determinar si la data se ha perdido o si ha sido alterada
Las señales de radio frecuencia o satelitales están expuestas a intercepción y/o inserción de información no autorizada	Un esquema de encriptamiento debe ser utilizado al enviar datos o información sensibles
La falla de un carrier local puede ocasionar que quede aislado y no pueda enviar importante información	Debemos considerar establecer medidas alternas que nos permitan hacer un By pass sobre el carrier local
Falla en el proceso de prioritización y selección de procesos alternos, atrasan el tiempo de recuperación	Todas las aplicaciones críticas y sus transacciones deben ser detectadas y cada seis meses probar la efectividad de los procesos de contingencia
Debemos ponderar muy bien los costos que supone el tener tecnología obsoleta o ser pioneros en el uso de nuevas tecnologías	Se requiere un estudio basado en las matriz de auditoria de IT cada dos a tres años que determine si pueden reducirse los costos sin sentir impactos negativos en los niveles de servicio.

2.2 Alternativas de Comunicación tal vez uno de los mayores problemas que tenemos en nuestras instituciones provienen de una facilidad que otorgamos con mucha facilidad y muchas veces sin justificación, nos referimos a "dial up", lo que se convierte en una excelente puerta de entrada para un Hacker, sobre todo por la facilidad que hay para conseguir "Demon Dialers" en Internet, nosotros en pruebas locales hemos utilizado con gran éxito *Tone Locator*(Toneloc), una táctica que hemos utilizado supone tomar una tarjeta de presentación y con ello tratamos de identificar el rengo de teléfonos al cual debemos llamar, que generalmente se encuentra ubicado entre el teléfono de la oficina y el del fax, la segunda fase parte de que conociendo el sistema operativo tratamos de utilizar los passwords que por defecto la aplicación o el sistema operativo nos da, aspecto que podemos conseguir en cualquier publicación de Hackers, el éxito en adivinar el password a través de un ataque de *"Fuerza Bruta"*, dependerá de las políticas de control de acceso que nos dan los sistemas operativos y que en la mayoría de los casos permite que la comodidad del administrador favorezca al Hacker, puesto que le permite gran número de intentos sin suspender la clave. La verdad es que los sistemas y aplicaciones en su gran mayoría nos dan muy buenas alternativas de seguridad, pero preferimos no leer los manuales y dejamos opciones sencillas y aun en algunos casos dejamos las que por defecto el sistema trae, esto es todo lo que necesita un Hacker o un auditor para detectar debilidades. Otra técnica que utilizamos con éxito es la utilización de un software de control remoto, que al igual que en los casos anteriores utiliza Dial Up, para ello instalamos en el recinto un producto (en nuestro caso *PC Anywhere*) esto nos permite llamar desde un área remota, conectarnos al PC y desde el acceder el host

2.2.1 Circuitos Dedicados o Rentados? Los circuitos rentados son una vía económica que nos permiten construir una red, pero al momento de tomar esta decisión debemos tomar en cuenta que los circuitos sub utilizados suponen un gasto excesivo en muchos casos, pero si el circuito es sobre utilizado tendremos una degradación en la red. Es muy importante por tanto para tomar cualquier decisión un monitoreo constante en la red, es muy importante determinar usos no convencionales tales como incrementos en tráfico sin explicación alguna, otro aspecto que debemos tomar en cuenta es que toda data crítica debe ser encriptada, por tanto si bien los circuitos rentados suponen poseer una red a corto plazo, supone además una extrema supervisión a fin de evitar que pasemos malos ratos

2.2.2 Medio de Transmisión dentro de las alternativas que tenemos una es muy importante y probablemente es la base sobre la cual sustentamos el esquema comunicacional es la capa 1 del modelo "OSI" la capa física, de ella debemos destacar el cableado como una base, el medio más difundido por supuesto es el *cable coaxial* el primer riesgo que apreciamos en el es la facilidad de ser interceptado, al igual que la facilidad con que se puede desviar la comunicación a un tercero. Otro esquema que por su reducción de costo y confiabilidad surge como una solución a corto plazo es *fibra óptica* dentro de las muchas ventajas que pudiéramos enumerar tenemos la alta velocidad que puede alcanzar, esta relativamente libre de errores, su mantenimiento es mínimo por no decir despreciable y su alta durabilidad, todas ellas lo ponen como una solución que tenemos a la vuelta de la esquina, pero su gran desventaja proviene de su propia ventaja, si el cable es cortado, se deja fuera de servicio a amplias áreas no sólo ya en el área de datos debemos incluir además voz y otros tipos de comunicación. A los anteriores debemos agregar *radio, microondas y satélites* todos ellos permiten esquemas de comunicación de alta confiabilidad, pero con una debilidad en común su fácil intercepción que nos lleva a concluir que este tipo de servicio siempre debe ser usado conjuntamente con un esquema de encriptación que de seguridad al medio ante la posibilidad de la intercepción

2.2.3 Programa de Auditoria el programa que utilizaremos esta enfocado básicamente a los siguientes aspectos:

- Identificar las alternativas de comunicación que se utilizan en la institución
- Identificar conexiones Dial up y determinar sus debilidades, mediante test de penetración
- Determinar debilidades para cada uno de los esquemas de comunicación que se utilizan
- Determinar la existencia de caminos alternativos para áreas críticas
- Revisar los esquemas de monitoreo que se utilizan y su efectividad
- Identificar circuitos sobre/sub utilizados
- Revisar la documentación de problemas y soluciones encontradas
- Determinar existencia de Plan de Contingencia, alternativas propuestas y efectividad

Matriz de Riesgos para Alternativas de Comunicación

Riesgo	Control
Pueden existir conexiones Dial up que desconozcamos	Utilizar periódicamente demon dialer que nos permitan identificar módems dial up no documentados Inspeccionar las estaciones y PCs a fin de determinar software de módems Monitorear mensajes de direcciones de IP que nos permitan detectar nuevas direcciones o desconocidas
Individuos no autorizados pueden acceder el sistema vía dial up	Utilizar tecnología de *call back*, en algunos casos podemos utilizar propiedades de los sistemas operativos o software como el *Defender II* para lograr el objetivo propuesto Utilizar técnicas secundarias de autenticación, que nos permitan determinar que el que se identifica es realmente quien dice ser
Los números telefónicos, Ids y passwords pueden ser compartidos, lo que permite accesos no autorizados	Monitorear el uso por cuenta e incluir filtros que permitan detectar exceso de uso
El uso de dial up debe ser restringido a fin de que sólo los estrictos necesarios puedan utilizarlo	Deshabilitar la autorización de dial up a todos los usuarios que no lo requieren
Los Hackers pueden penetrar a trayectos de redes rentadas	Monitorear estos circuitos y detectar tráfico inusual Active en los equipos las posibilidades de detección de direcciones y permite que avise por tráfico inusual o por nuevas direcciones
El costo de circuitos no utilizados supone un exceso en los costos	Identifique sub utilización en circuitos
Los errores en los circuitos degradan los tiempos de respuesta	Monitoree los circuitos y de forma proactiva detecte problemas que pueda presentarse, se recomienda el uso de herramientas como *HP-Openview, Tivoli, CA-Unicenter*
Data confidencial puede ser obtenida y utilizada por personas no autorizadas	Encripte toda la información confidencial
Fallas en el sistema de cableado puede ocasionar serios problemas en la productividad de las unidades de negocio	Mantenga todos los cables en los gabinetes y su ruta protéjala con cubiertas de protección
Elementos ambientales pueden ocasionar fallas en los circuitos	Tener rutas alternativas para información crítica
Mensajes no autorizados pueden ser recibidos y sobrecargar los circuitos	Establecer filtros que identifiquen los mensajes que se originan desde locaciones desconocidas Identificar y segregar archivos con sufijos exe, bat, com Monitorear volumen de mensajes entre locaciones
Información de relevancia puede perderse o dañarse en el proceso de transmisión	Utilizar secuencia de chequeo para este tipo de transmisión
El uso de nuevas tecnologías puede incrementar los costos e interrumpir el proceso del negocio	Utilice una tecnología probada siempre que pueda Aunque nuevas tecnologías ofrecen ventajas competitivas si no es requerido no se convierta en un conejillo de indias Trabaje con empresas reconocidas y que le den apoyo comprobado en caso de requerirlo

2.3 Internet y Redes Públicas Internet es probablemente la forma más expedita y con mayores éxitos conseguidos para penetrar una red, esto se esta logrando además de por el hecho de estar expuestos a todo tipo de ataque y desde cualquier locación al hecho de que convivimos con ella y tendemos a relajar las políticas volviéndonos complacientes, aspecto que los Hackers saben apreciar ya que les permite atacar libremente a cualquier institución inscrita en Internet y las Instituciones gubernamentales, universidades y empresas exitosas se han convertido en foco de ataques, a pesar de que muchas empresas han implantado *"Firewalls"* y establecido políticas de control, muchas veces la entrada que protege el *Firewall* no es la única entrada a la empresa, por tanto para proteger a la institución requerimos conocer todas las conexiones que tenemos con Internet, y Además reexaminar con mucho detenimientos el sistema operativo a fin de detectar debilidades que puedan ser utilizadas por aquellos que quieren accedernos.

2.3.1 Control al nivel del Firewall Probablemente el mayor problema que se nos presenta cuando trabajamos sobre Internet sea la ausencia de un Firewall o la presencia de uno sin políticas adecuadas o que no se ha probado de una manera suficiente para asegurara que lo propuesto sé esta cumpliendo, otro de los grandes problemas proviene de pasar sobre el Firewall utilizando esquemas de Dial up de una manera poco controlada, es necesario hacer ver al administrador el riesgo de no tener instalados los controles adecuados y para ello proceder con pruebas de penetración que le hagan comprender el riesgo que corre por no tener instalado un control adecuado. La falla más común que se encuentra es en el ámbito de Routers ya que en muchos casos no tienen detección de intrusos, damos tres veces el password y estamos fuera pero no queda registrado, en otros casos se esta usando el password que por defecto tiene el fabricante. Es importante recordar el control que los Routers llevan a cabo cuando configuramos un Firewall

2.3.2 Control al nivel del Sistema Operativo es esencial asegurar que el sistema operativo es seguro y que protege a todos los equipos que conforman el cluster que para los efectos de nuestro estudio incluye el Firewall, el Web Server y el FTP Server, lo primero que haremos será obtener la configuración de la red, en esta configuración debemos asegurarnos que esta presente el Sistema Operativo que utilizamos y los Servidores que operan en nuestra red, con esta configuración revisaremos cada máquina y aseguraremos que cumple con lo que la política de seguridad establece, una vez revisado estableceremos una política de Control de Cambio a objeto de asegurar que cualquier cambio que se realice de allí en adelante cumplirá con los requisitos de seguridad exigidos. Dado que estamos utilizando básicamente NT como sistema operativo desde el "User Managers for Domains" recomendamos establecer una política como la que mostramos a continuación:

Password Restrictions
Maximum Password Age... Expires in 35 Days
Minimum Password Length... At least 8 Character
Minimum Password Age..... Allow changes immediately
Password Uniqueness... Remember 24 passwords
Account Lock out
Lockout after... 3 bad logon attempts
Reset count after 500 minutes
Lockout duration... forever until admin unlocks

Además de las especificaciones que hemos establecido para el control de acceso, un Segundo elemento debe ser agregado en el esquema básico de seguridad que hemos indicado y es el elemento que nos permita hacer un seguimiento de lo que ocurre por medio de los logs, todas las fallas que se presenten deben ser grabadas, de esta manera aseguramos que cualquier intento de violar la seguridad quedará registrado, aquí de igual manera garbaremos cualquier cambio en la configuración que se lleve a cabo de esta manera aseguramos que al política de Control de Cambio funciona de manera precisa. Los elementos que monitorearemos son los siguientes:

Auditar estos Eventos	Exito	Falla
Logon y Logoff		X
Acceso a Archivos y objetos		X
Uso de derechos de usuario		X
Usuario y su Grupo	X	X
Cambio en políticas de Seguridad	X	X
Cancelación y Rearranque del sistema	X	X
Seguimiento del Proceso		X

Políticas similares podemos utilizar independientemente del sistema operativo, lo importante de ello estriba en tener un buen esquema de acceso, además de asegurarnos que quedan registradas las acciones que se cometen contra el sistema, es nuestro deber además establecer filtros que nos permita por defecto acceder a los logs y distribuir el log a los Administradores de Descentralizados a fin de que los usuarios conozcan quienes están utilizando al información que administran y porque se han intentado accesos que han sido denegados

Aunque tenemos diversos logs de firewalls ya que los mismos varían de acuerdo al vendedor, los reportes que hemos podido observar reportan el mismo tipo de alertas con diferentes mensajes, de igual manera nos presentan en promedio 25 megabytes de longitud ya que registran todas las acciones que acontecen, reportes de tal magnitud difícilmente pueden revisarse, por tanto pasamos los reportes a archivos planos, procedemos a sortear los logs y únicamente revisamos los mensajes de warning o de categoría superior. Un elemento adicional recomendamos y es por un procedimiento similar tratar de conocer a donde van de visita nuestros usuarios

Podemos concluir con la siguiente recomendación, todas las conexiones a Internet deben estar protegidas por un Firewall, el sistema operativo debe estar configurado de manera segura y constantemente monitoreado, los log generados por Routers y Firewall deben ser revisados diariamente, debemos instalar software antivirus(*Norton o Mcafee*) y software que permita detección de intrusos al nivel de Firewall a este nivel recomendamos(*RealSecure de IIS, Intruder Alert de Axent, Webstalker de Haystack*), de igual manera es muy importante que al menos una vez al año hagamos pruebas de penetración, dentro de esta prueba es muy importante que conozcamos nuestra fortaleza frente a ataques de negación de servicio, en poco tiempo que hemos venido observando hemos detectado 5 ataques a la institución usando este método, los mismos han sido descubiertos por el inusitado incremento en el ancho de banda observado en horas poco usuales. Por último es muy importante desarrollar una política de uso de Internet a objeto de que nos se abuse de este instrumento

2.3.3Programa de Auditoria el programa esta orientado a la identificación de riesgos derivados de Internet y cubre los siguientes aspectos:

- Identificar las conexiones con Internet
- Crear un diagrama del cluster de Internet, en el se deben mostrar los equipos, las direcciones IP y las conexiones con la Intranet
- Identificar las políticas de Internet y determinar su cumplimiento
- Establecer procedimientos que nos conduzcan al uso del medio de manera segura
- Educar a los usuarios y mostrar los riesgos que supone el mal uso de Internet
- Determinar el grado de seguridad de los servidores que se están conectando directamente a Internet
- Determinar si hay conexiones a Internet fuera del ámbito protegido por los firewalls
- Identificar y establecer procedimientos que tiendan a erradicar archivos poco seguros ubicados en el cluster de Internet

Matriz de Riesgo para Internet

Riesgo	Control
Las autoridades no conocen los riesgos implícitos de Internet y no toman precauciones que permitan defender la integridad de la red o la institución	- Crear una política de acceso a Internet que sea fácil de asimilar. Que proporcione claridad en lo que puede llevarse a cabo y lo que no puede hacerse y asegurara que esta política sea difundida en toda la comunidad - Establecer procedimientos que permitan detectar violaciones a estas prácticas
Los usuarios abusan en la utilización de Internet y como consecuencia de ello se pierde productividad, se incrementa la carga en los circuitos, se deteriora el tiempo de respuesta	Monitorear los accesos a Internet, crear perfiles de usuario que nos permitan detectar desviaciones. Alertar a los usuarios que presentan desviaciones y tomar acciones disciplinarias frente a acciones de constante violación
Intromisión de Hackers o conexiones poco seguras	-Utilizar firewalls a fin de reducir la posibilidad de penetración a la red por personal extraño -Asegurar que todo acceso a Internet se hace vía Firewall - Utilizar cuentas en router y firewalls que nos permitan identificar volúmenes poco usuales de información
No se usa un scanner de virus al nivel de firewalls y servidores de Internet	Instalar un escáner que permita la detección de virus antes de que infecte la Intranet
No se puede identificar intentos de penetración, pues hay gran cantidad de visitantes que tratan de acceder el medio	Instalar herramientas que de manera activa hagan seguimiento a intentos de penetración
Cambios no autorizados llevados a cabo en la página Web, motivado a que los archivos CGI (Common Gateway Interfaced) no están propiamente protegidos	Asegurar mediante el sistema operativo que estos archivos no pueden ser accedidos
Se usa Telnet, FTP y tftp para penetrar la red	Revisar el sistema operativo y detectar todos los sistemas que se conectan a la red pública o que puede acceder la red pública a través de otras redes. Asegúrese que tftp (trivial file transport protocol), asegurar que todas las cuentas existentes están identificadas y poseen password
Como los Emails, archivos y transacciones pueden requerir usar la red pública y por tanto pueden ser observadas, modificadas	Esta información debe ser encriptada para ello podemos utilizar recursos de muy bajo costo y en muchos casos distribuidos gratuitamente tales como *Viacrypt, PKZIP y Winzip.* En el caso de transacciones financieras es recomendable el uso de *SET*
Ubicamos servidores fuera del ámbito del Firewall para que pueda ser accedido por entes externos. Los Hackers pueden aprovechar esta circunstancia	Asegurarse a diario que la información es revisada, identificar si existe algún tipo de información crítica en estas locaciones, asegure eliminar los archivos que no son requeridos e identifique cualquier archivo nuevo que se haya creado.
La seguridad se degrada accidentalmente, lo que permite a potenciales Hackers ingresar a la intranet	Deben llevarse a cabo de manera sorpresiva pruebas de penetración
Constantemente nuevas técnicas aparecen que hacen que lo que creíamos seguro se torna inseguro	Revise con cierta frecuencia los alertas de *CERT* y asegúrese que los patches que nos remiten los suplidores son instalados prontamente

2.4 Operación y Gerencia de Redes la necesidad de un personal preparado para la operación y la Gerencia de las Redes es un ingrediente fundamental para tener una red segura. Si la operación de la red no es la más apropiada tendremos una red degradada y que al final pude convertirse en una red inmanejable. La tecnología de red esta cambiando muy rápidamente, lo que supone una carga adicional en la gerencia de red ya que deben hacer un constante seguimiento en el desarrollo de nuevas tecnologías.
El personal especializado, crea otro problema para esta gerencia, las universidades no están preparando a este tipo de personal, y las posiciones que se ofrecen en muchos casos no son muy atractivas para los nuevos graduados, aquellos que finalmente se deciden por esta área, les espera una curva muy larga de aprendizaje antes de comprender las complejidades que la red supone y su evolución. Retener a este personal de igual manera se convierte en un reto ya que su especialidad es escasa en el mercado y constantemente este personal es tentado por otras empresas a fin de hacerse con sus servicios.
Es muy difícil explicar al resto de los gerentes que conforman el grupo de sistemas la dificultad que supone este tipo de posición, la misma no se basa únicamente en los conocimientos aprendidos en el área académica, supone además una experiencia que en muchos casos implica una o dos décadas y si quisiéramos definir a este tipo de profesional deberíamos catalogarlo como alguien que conoce las técnicas, tiene experiencia, energía y alta motivación, características estas muy difíciles de encontrar.
Desde el punto de vista de la operación y seguridad de la misma, uno de los principios que debemos tomar en cuenta es la disponibilidad de la información y la continuidad operativa, para ello los siguientes elementos adquieren una primordial importancia:

- El Plan de Contingencia
- Mantenimiento preventivo y correctivo
- Políticas de Control de Cambio
- Establecimiento de Niveles de Servicio
- Operación de la red
- Detección proactiva de problemas
- Nuevas tecnologías
- Soporte a los Sistemas Operativos
- Instalación de nuevos equipos

2.4.1 Reportes de la Gerencia la gerencia requiere información de manera de lograr el personal requerido, mantener los niveles prometidos y obtener los requerimientos presupuestarios. Para poder cumplir una serie de reportes deben llegar a sus manos y con ellos tomar las decisiones que su posición suponen ellos son:

- Utilización de la red por segmento
- Disponibilidad de cada segmento
- Estadísticas de niveles de servicio
- Restricciones operativas y de red
- Planificación a corto y mediano plazo
- Costos y presupuestos operativos

La obtención de esta información requiere de una serie de paquetes que permita la obtención de la información para ello requiere de una serie de elementos de software que le permitan obtener la información y tomar las decisiones que su posición exige, es muy importante mantener el criterio que en el análisis de la información utilizará parte de ella para acciones inmediatas y otra para la planificación y toma de decisiones referente a la tendencia que la institución debe seguir

2.4.2 Programa de Auditoria la auditoria que detecte el cumplimiento de esta función esta basada en los siguientes aspectos:

- Revisar los riesgos que mostramos en los segmentos anteriores
- Determinar si existen riesgos adicionales que no se hayan detectado
- Revisar la información gerencial y determinar si la misma cubre todos los aspectos necesarios para el cumplimiento de las funciones de la posición
- Mantener de manera precisa los reportes de análisis de riesgo y determinar las medidas que contribuyen a su mitigación
- Probar el Plan de contingencia y asegurar la disponibilidad de ,los elementos requeridos para su éxito

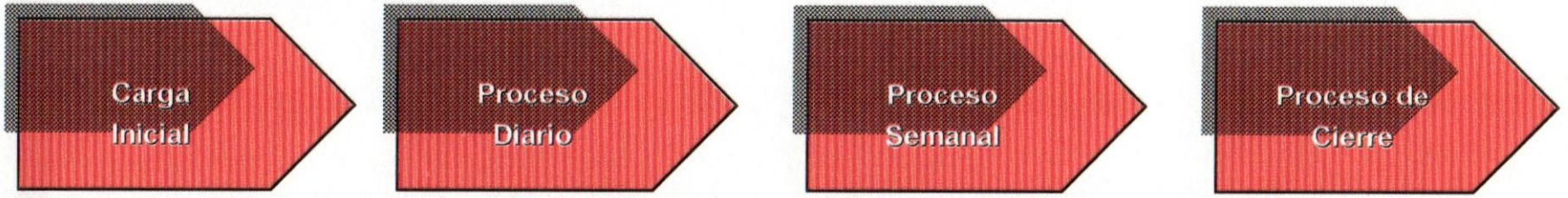
Matriz de auditoria para la función

Riesgo	Control
Si la edificación desaparece, la institución sé vera privada del servicio de red	La institución exigirá a la gerencia de operaciones el cumplimiento con el Plan de Contingencia, el mismo cubrirá los servicios críticos de red
Un simple punto de falla puede ocasionar una gran interrupción del servicio de red	Un grupo técnico debe revisar los componentes de red y determinar las necesidades que estos equipos requieren para cumplir con su cometido, para cada elemento crítico que soporte un elemento imprescindible de red, se buscaran soluciones que mitigue el riesgo encontrado, se establecerá un procedimiento de recuperación y se probará su eficaz funcionamiento. Se establecerá redundancia de equipos críticos De ser necesario y de acuerdo con la criticidad del sistema se establecerán esquemas de contingencia que se cumplirán en el tiempo de acuerdo con lo pautado en los niveles de servicio acordados entre la institución y la gerencia de sistemas
En caso de una contingencia las funciones críticas de la institución fallan y como resultado se ocasiona la interrupción de las funciones críticas	Debe estar funcionando y probado un Plan de Contingencia, el mismo será tempo dependiente, recuperando cada una de las funciones críticas de acuerdo a lo establecido en el nivel de servicio ofrecido. El Plan será probado al menos dos veces al año, estará relacionado con el esquema de Control de Cambio y si un cambio afecta algún proceso establecido en el Plan de Contingencia, el mismo será sometido a revisión y prueba a fin de constatar su eficacia
Sin un mantenimiento efectivo la efectividad de la red se vera disminuida y potencialmente podrá llegar a situaciones críticas y/o largas interrupciones	Deben establecerse procedimientos que aseguren que todos los elementos críticos de red tengan su apropiado mantenimiento, conforme a las especificaciones del equipo y las necesidades expresadas por los suplidores El personal operativo se asegurará que el mantenimiento ofrecido se lleva a cabo acorde con la norma del equipo, y que la calidad del trabajo que lleva a cabo el personal de mantenimiento cumple o excede el mínimo de estándares establecidos
El personal de mantenimiento puede resultar lesionado mientras cumple con sus funciones, puede tener acceso a información crítica o confidencial, puede alterar información crítica, instalar equipos no autorizados o hacer monitoreo no permitido	Todo personal de servicio o apoyo debe ser supervisado mientras están cumpliendo con sus funciones. Sólo personal autorizado tendrá acceso a las áreas críticas de red, serán supervisados por personal entrenado y que conoce las actividades que el personal de mantenimiento llevará a cabo. Debe existir una orden de trabajo o un reporte de falla para cada una de las labores que lleva a cabo el personal de mantenimiento Si el personal de mantenimiento no programado, el mismo debe ser confirmado por el grupo supervisorio del suplidor, debe registrarse el inicio, fin y los equipos que fueron alterados
Sin registros de mantenimiento es imposible monitorear la efectividad del mantenimiento, de igual manera no podremos determinar problemas repetitivos	Debe mantenerse un registro de todos los elementos de hardware y software, debe establecerse en el contrato de servicio elementos escalares que permitan después de cierto tiempo escalar a organismos superiores, deben establecerse penalidades en el contrato

El retardo en el reporte de una falla puede incrementar el daño que sufre un equipo, retardar operaciones críticas o degradar la productividad	Deben establecerse procedimientos que permitan reportar cualquier tipo de falla o problema y acelerar la pronta recuperación Debe buscarse un sistema que automatice el reporte de problemas y debe informarse al Help Desk a cerca de las implicaciones del mismo A través de este esquema debemos determinar los problemas repetitivos y buscar la causa y solución encontrada Estos reportes incluirá los tipos de problema que se ha detectado, el producto afectado, el MTBR, los problemas repetitivos y otros ítem que sirvan para hacer seguimiento a los problemas
Problemas al momento de carga de la red, pudieran resultar en un deterioro del tiempo de respuesta	Debe establecerse procedimientos de carga, análisis y balanceo de cargas en al red, eliminar circuitos que no son requeridos, hacer seguimiento con programas de monitoreo y determinar potenciales problemas
Personas extrañas pudieran intentar penetrar la red, incrementar el tráfico de red, incrementar los costos al utilizar segmentos o ancho de banda adicional, deterioro en el tiempo de respuesta	Debe monitorearse constantemente la red, la supervisión y los mensajes de SNMP deben ser capturados periódicamente para asegurar que estos mensajes se originan internamente en la red o desde una fuente autorizada fuera de la red El monitoreo de la red debe incluir la revisión de la posible existencia de monitores externos que envían mensajes a la red, estos deben ser investigados y prontamente removidos
Las redes pueden crecer por accidente resultando en incremento de costos y pérdida de productividad	Debemos a través del monitoreo determinar tendencias y hacerles seguimiento Los reportes gerenciales deben prepararse a fin de obtener tendencias de crecimiento, uso, tendencias y cumplimiento con lo establecido en los niveles de servicio El análisis base cero debe hacerse periódicamente a fin de identificar uso superfluo de recursos
La implantación de aplicaciones nuevas, de repente ocasiona una sobrecarga en la red, ocasionando una degradación en el servicio y en algunos casos dejar a la institución sin los servicios de red	Los analistas de redes deben conocer a través de los esquemas de Control de Cambio de cualquier variación en los servicios de red, cualquier cambio dentro de lo posible debe ser simulado en laboratorio, si después de ello todavía se presentan fallas alternativas deben estar presentes que permitan volver a las situaciones originales Anualmente debe conocerse acerca de los nuevos requerimientos de las organizaciones a fin de analizar el impacto que tal servicio supone para la red

Identificación de Procesos Por Organización

Producto Administración
Procesos:Contabilidad

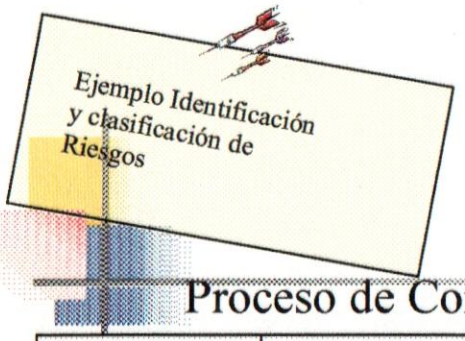


- **Auditoria Interna**
- **Ctas x Pagar**
- **Ctas x Cobrar**
- **Nóminas**
- **Costos**

- **<u>Sistema Backoffice</u>**
- **Establece balance diario**
- **Controla subcuentas daily flash**
- **Analiza rechazos, detecta herrores y efectua correcciones**

- **<u>Analiza Cuentas</u>**
- **Produce estado financiero semanal(weekly)**
- **Analiza informe con Contralor**
- **Presenta informe a Jefes de Dpto.**
- **Analizan en conjunto desviaciones**
- **Hacen correcciones**

- **<u>Weekly</u>**
- **Completado análisis y correcciones**
- **Estado financiero mensual**
- **Analiza con contralor**
- **Envia a Administradora**
- **Administradora Revisa**
- **Emite ajustes y correcciones**
- **Estado financiero mensual final**
- **A fin de año produce cierre anual**



Análisis de un Proceso

Proceso de Contabilidad

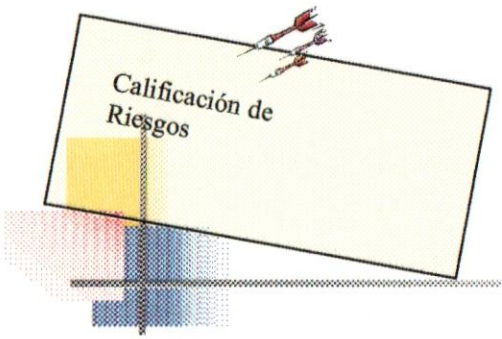
Proceso	Evento	Riesgo	Tipo Crisis Neg	Ext	Mer	Prob Ocurr	Valor	Impacto	Ident de Criticidad	Suplidores Externos
Revisión de Carga y proceso diario	•Auxiliar de cuentas generado por auditoria •Auxiliar de Cuentas por cobrar •Auxiliar de Cuentas por pagar •Caja principal •Comprobantes de Nómina •Comprobante de Costos	•No se registra la información	●			•Medio	• 4	• 2	Medio (18)	•CANTV •Electricidad de Caracas •HP •Microsoft •Sistema Activo •Personal Contratado •Domesa •Equipos de Fax y Fotocopiado •Operadora •Banca local e Internacional
		•Sistema CLS o Back Office no funcionan y se retrasa contabilidad	●	●		•Alto	• 9	• 3		
		•Integridad de datos	●	●		•Alto	• 8	• 2		
		•Retraso en cobranzas	●			•Alto	• 6	• 2		
		•Auxiliares no balanceados	●			•Medio	• 8	• 3		
		•Mal posteo	●			•Medio	• 7	• 3		
		•Errores en nómina				•Alto	• 5			
		•Problemas en balance diario por fallas de sistema o actualización	●			•Medio •Alto	• 8 • 6	• 2 • 3		
		•Sub cuentas no reflejan actividad real	●			•Alto	• 7	• 3		
		•Mal analisis y posteo erroneo en correcciones, desbalanceo de resto de cuentas	●			•Alto	• 6	• 3		
		•Fallas en cierre semanal	●			•Alto •Alto	• 8 • 7	• 2 • 2		
		•Decisiones erradas basadas en cálculos inexacto	●	●		•Alto	• 4			
		•Seguridad del sistema no permite integridad de información	●			•Medio •Alto	• 7 • 7	• 3 • 3		
		•Fallas en respaldo, producen desbalance en información	●			•Alto •Alto	• 6 • 7	• 3 • 3		
		•Pérdida de respaldo de transacciones no permite reconstruir información	●			•Alto		• 2		
		•Fallas de comunicación con banca local y con tesoreria								

Anexo 2 Figura 4

Elementos Mitigadores

Proceso de Contabilidad

Proceso	Riesgo	Tipo Crisis			Prob Ocurr	Valor	Impac	Elementos Mitigadores
		Neg	Ext	Mer				
Revisión de Carga y proceso diario Medio (18)	•No se registra la información	●			•Medio	• 4	• 2	•Si CLS o Back Office, no funcionan correctamente, con el plan de respaldo instituido puede recuperarse la información ya que las transacciones se mantienen respaldadas, en caso de detectarse corrupción en la información, se partiría de la última información no corrupta y las transacciones que durante el lapso transcurrido han sido sometidas, de esta manera se recuperará la información •La integridad de los datos se garantiza por los procesos de respaldo diario de transacciones y su subsecuente proceso, el de respaldo de los archivos de las aplicaciones, conjuntamente con el plan de recuperación. Todos estos procesos se encuentran descritos en los procesos de contingencia y están dentro de los procesos de producción del centro. •Los problemas de servicio son responsabilidad de mantenimiento, al momento se están tomando las previsiones necesarias, pero el área de Contraloría, no recibe este servicio, por tanto la Auditoria se procesará en el Centro de Computación •Los problemas de la comunicación se lleva a cabo a través de la central telefónica, por tanto cualquier problema que pudiera surgir de ser solucionado o mitigado con el Plan de Contingencia de la Central Telefónica (Responsable Computación), pero pudiera presentarse una falla en la recepción de tarifas via Internet, por lo que se sugiere establecer los procedimientos que aseguren la recepción de la transmisión utilizando medios alternos . •En los procesos de Contingencia se establece el procedimiento para subsanar los problemas de nómina que pudieran presentarse, el mismo ataca la corrección por de datos por problemas de posteo, por problemas de cálculo y por tanto corrupción de la data y por falla en el proceso que impiden la ejecución del sistema. •Se sugiere establecer un plan de seguridad en el que se pueda establecer claramente la responsabilidades de cada puesto y auditar el archivo a fin de detectar cualquier alteración de la información y establecer las sanciones necesarias, además de lo anterior expuesto es requerido el establecimiento de políticas de control de cambio que oficialicen la ejecución y cambios en los procesos o programas(Responsable Computación)
	•Sistema CLS o Back Office no funcionan y se retrasa contabilidad	●	●		•Alto	• 9	• 3	
	•Integridad de datos	●			•Alto	• 8	• 2	
	•Retraso en cobranzas	●	●		•Alto	• 6	• 2	
	•Auxiliares no balanceados	●			•Medio	• 8	• 3	
	•Mal posteo	●			•Medio	• 7	• 2	
	•Errores en nómina	●			•Alto	• 5	• 3	
	•Problemas en balance diario por fallas de sistema o actualización	●			•Medio •Alto	• 8 • 6	• 2 • 3	
	•Sub cuentas no reflejan actividad real	●			•Alto	• 7	• 3	
	•Mal analisis y posteo erroneo en correcciones, desbalanceo de resto de cuentas	●			•Alto	• 6	• 3	
	•Fallas en cierre semanal	●			•Alto	• 8	• 2	
	•Decisiones erradas basadas en cálculos inexacto	●			•Alto	• 7	• 2	
	•Seguridad del sistema no permite integridad de información	●	●		•Alto	• 4	• 3	
	•Fallas en respaldo, producen desbalance en información	●			•Medio •Alto	• 7 • 7	• 2 • 3	
	•Pérdida de respaldo de transacciones no permite reconstruir información	●			•Alto •Alto	• 6 • 7	• 3 • 3	
	•Fallas de comunicación con banca local y con tesoreria	●			•Alto		• 2	



Dimensión del Riesgo

Probabilidad de Ocurrencia

Definitivamente Ocurrira = 1
Alta posibilidad de Ocurrencia = 0.7
Posibilidad Moderada = 0.4
Posibilidad Remota = 0.2

X

Impacto

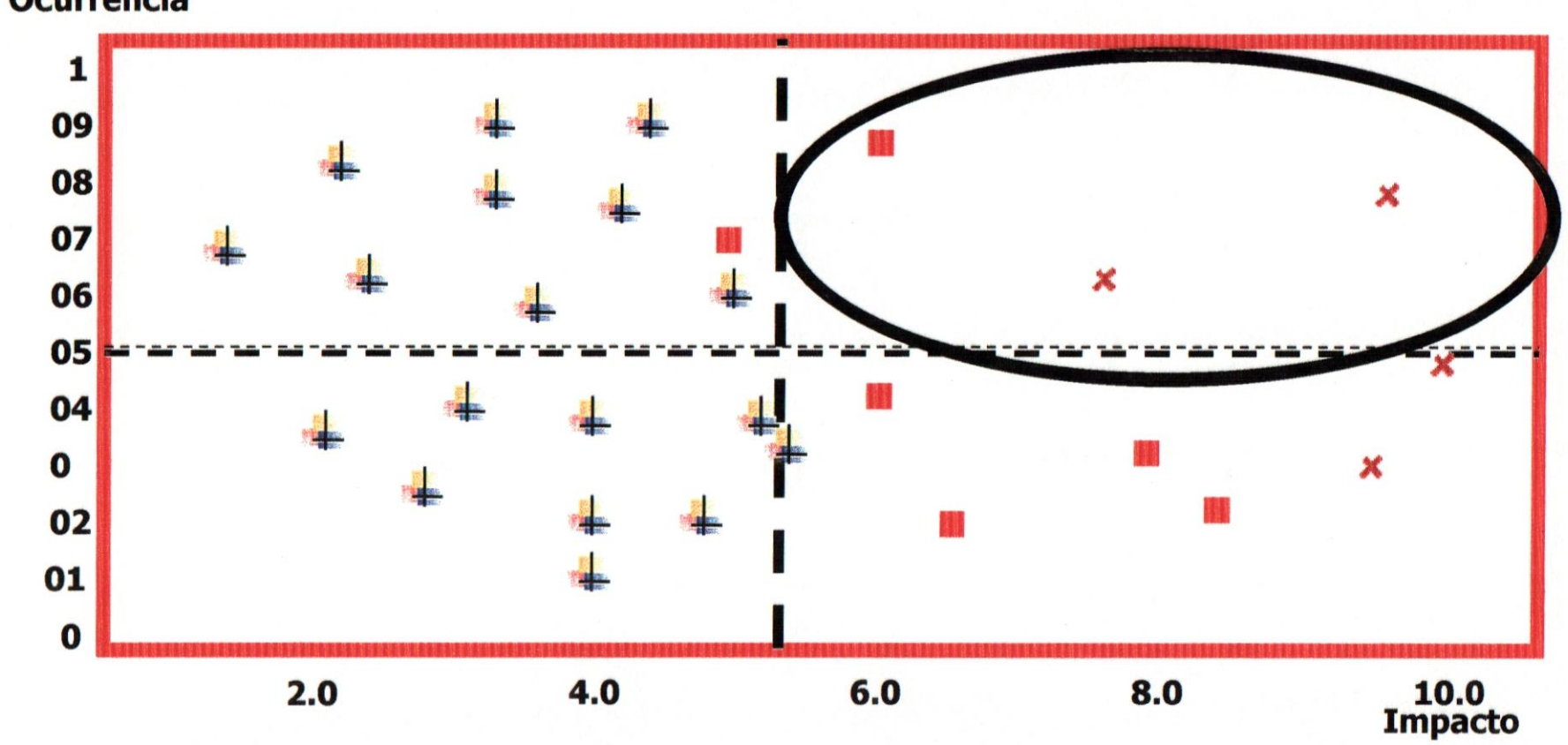
Alto 10
Medio 5
Bajo 1

=

Dimensión Del Riesgo

Dimensión del Riesgo

Calificación de Riesgos



Fuentes de Riesgo

3 El Reporte de Riesgo al momento hemos conformado toda una información operativa, que sumada a la información propia de las aplicaciones nos permitirá llegar a una información de riesgo y de los esquemas de mitigación que actuaran en cada uno de los casos, el procedimiento a seguir es el siguiente:

3.1 Identificación de Procesos por Organización supone mantener una reunión con los diferentes entes que de una forma u otra tienen que ver con la información que se esta suministrando a la organización, de esta reunión obtendremos un reporte que nos muestra los objetivos de la organización, los servicios que ofrece a los usuarios, que unidades constituyen la organización y que servicios como informática les estamos ofreciendo, un ejemplo práctico podemos observarlo en el ***"Anexo 2 Figura 2"***, en el mismo hacemos seguimiento a una organización que es la de Administración y a sus procesos, y posteriormente explotamos cada uno de los procesos

3.2 Análisis de Proceso una vez identificados los procesos, pasamos a realizar el proceso de explotar los eventos que intervienen, para esto realizamos una reunión conjunta entre los usuarios, los analistas de mantenimiento y la gerencia de operaciones, el primer paso que seguimos es determinar los eventos que se dan en los cuales interviene la Gerencia de Sistemas, una vez identificados los *eventos* pasamos a hacer un análisis sobre los *riesgos* involucrados para cada uno de los procesos, completado este paso tratamos de identificar el *tipo de crisis* que se presenta, esto lo hacemos para establecer el grado de control que tenemos sobre el problema, si la crisis es interna, la solución al problema esta en nosotros, pero si la misma depende del suplidor o aun más si depende de políticas externas o de alto gobierno, la solución trasciende de las soluciones que podamos encontrar, a manera de ejemplo podríamos establecer un proceso automatizado para el control de respaldo que nos hemos dado cuenta que por errores de los operadores se han venido sucediendo y solicitar a contraloría a través del presupuesto anual la automatización del proceso, pero si el gobierno decreta una devaluación tenemos que revisar el presupuesto o atrasar la solución propuesta. El siguiente aspecto tiene que ver con la *ocurrencia del problema detectado* esto lo hacemos sobre la base de la experiencia del panel que ha concurrido, es un método esencialmente intuitivo pero la experiencia del panel nos indica que la información tiende a ser bastante acertada, de todas maneras esta información se contrasta con las estadísticas que la Gerencia de Redes posee lo que corrobora la información obtenida o nos permite contrastar la información que nos da el usuario contra la realidad estadística obtenida y reflejar finalmente la realidad mediante un consenso. Una vez llegamos a un consenso, damos un valor que va de 0 a 10, ese valor refleja el peso que representa la presencia de la falla analizada para el proceso si la falla no me permite continuar o supone un retraso en el proceso, podríamos decir que su valor esta entre 7 y 10, pero si no altera el proceso le daremos un valor de 0 a 3. El *impacto*, viene dado por el valor que obtuvimos en la probabilidad de ocurrencia, buscamos obtener de esta manera un valor que multiplicado por el valor nos indique la *criticidad* , el valor máximo que podremos obtener es 30 que vendría dado por un valor 10 y un impacto 3, los valores obtenidos los promediamos y obtenemos la criticidad del proceso. Por ultimo identificamos los entes *externos* esto nos permite identificar que entes intervienen y como podemos negociar con ellos a fin de evitar el impacto negativo que su ausencia pudiera ocasionar en el proceso que analizamos. En el ***"Anexo 2 Figura 3"*** podemos observar un ejemplo de un análisis de proceso

3.4 Elementos mitigadores del análisis realizado anteriormente, detectamos una serie de problemáticas que pueden ser solucionadas de inmediato y por tanto solventar la problemática que hemos analizado, para ello buscamos soluciones que mitiguen el riesgo detectado y disminuyan la probabilidad de ocurrencia en la problemática que hemos descubierto, el ***"Anexo 2 Figura 4"*** nos muestra los mitigadores propuestos para la problemática que hemos detectado

3.5 Dimensión del Riesgo del paso anterior tendremos una serie de soluciones para la problemática que hemos analizado conjuntamente con el usuario, pero parte de las soluciones no satisfacen de una manera completa los requerimientos exigidos para obtener una solución de calidad acorde con las necesidades de la institución, bien sea por que la solución es parcial o porque no hemos encontrado una solución que mitigue el problema que se ha presentado, razón por la que debemos ir a una instancia superior con los casos que siguen pendientes a la espera de un mitigador.
Completado el análisis de todos los procesos y obtenidos los valores de criticidad, hacemos un análisis del proceso no mitigado y lo contrastamos contra la criticidad que tiene para la continuidad de la empresa, previamente la institución estableció la política que nos permita identificar la dimensión del riesgo, en ella

valora el impacto que tiene el proceso contra las operaciones globales de la empresa en nuestro caso específico obtenemos los siguientes valores:

Valor del Riesgo	Impacto
7 a 10	Peligro de vidas, salud, paralización total de la empresa, pérdida masiva de clientes, perdida de confianza
4 a 7	Retraso significativo en la operación, posibles demandas, corrupción de la información, obtención de datos imprecisos
0 a 4	Perdida de oportunidad de negocios, inconveniente a clientes, baja de fluidez, retraso leve en los procesos

El valor del riesgo lo multiplicamos por la probabilidad de ocurrencia lo que nos da la dimensión del riesgo, tal como lo podemos observar en el ***"Anexo 2 Figura 5"*** y obtenemos la gráfica de "Dimensión de Riesgo", ella nos da una indicación acerca de los procesos que de acuerdo con el análisis basado en las políticas de la empresa, debemos avocarnos prontamente y cuales pueden esperar, ver **"Anexo 2 Figura 6"**

3.6 Limitaciones del Proceso. Las limitaciones del proceso vienen dadas por el control que podamos tener sobre el proceso, si la solución esta dentro del ámbito de la empresa no tendremos inconveniente para solucionar la problemática que hemos encontrado, pero en la medida que salimos del ámbito de la empresa, vamos perdiendo control y dependemos de soluciones negociadas, pero además hay medidas o efectos que dicta el país o la economía mundial y que de una manera u otra afecta a los procesos y por ende disminuyen la posibilidad de solución, a través de la figura que presentamos en el "***Anexo2 Figura 7***", indicamos las limitaciones básicas que hemos propuesto a lo largo de este anexo.

4.0.Herramientas Automáticas de Análisis de Riesgo existe una gran variedad de herramientas que permiten llevar a cabo un análisis de riesgo en una institución, pero tenemos con ellas un serio problema y es que las mismas miden riesgos específicos de zonas o países y por tanto para poder aplicarlo se requiere un proceso de tropicalización, a manera de ejemplo tomemos el riesgo Terremoto, dentro de un mismo país como lo es USA, hay una gran variación en la apreciación del riesgo en la costa del Pacífico y la del Atlántico.

ARES
@RISK
BDSS
Control Matrix Methodology
COSSAC
CRITI-CALC
GRAMM
GRA/SYS
IST/RAMP
JANBER
LAVA
LRAM
MARION
Micro Secure Self Assessment
Predictor
PRISM
QuickRisK
Ra/Sys
RANK-IT
RISKCALC
RISKPAC
RISKWATCH

Anexo 3

Respaldo Recuperación y Administración de Almacenamiento

Lineamientos Generales debe iniciarse un proyecto para lograr un esquema de Administración de Almacenamiento Respaldo y Recuperación (RR/AA), lineamientos similares a los que se han manejado en los esquemas de almacenamiento centralizado, pero con la diferencia que en un ambiente distribuido se transforma en básica, la dispersión geográfica que nos ofrece una visión diferente de la manera de enfocar el problema. Dispersión no puede ser casual para que la información requerida no puede hacerse disponible, por tanto debemos buscar la manera de dar adecuada protección y respaldo a la información independientemente de donde la misma se encuentre. Tradicionalmente la obtención y custodia de respaldos ha estado circunscrita al área de informática, igual debe continuar en los ambientes distribuidos sin que esto implique un aumento en los recursos(horas hombre) invertido para ello. De la misma forma, el vertiginoso crecimiento en los requerimientos de almacenamiento supone una eficiente administración que permita optimizar y balancear el uso de la pirámide de almacenamiento. Esta necesidad nos lleva a recomendar la automatización y centralización de las funciones de RR/AA

Tendencias tecnológicas los requerimientos de ubicaciones adecuadas y controladas para los esquemas RR/AA, es común para todos los profesionales de computación no importando el tipo de esquema en el que se este operando, la razón es simple, las organizaciones sin importar el tamaño de las mismas no pueden correr el riesgo de que la información requerida en un instante, no se encuentre disponible. De hecho sería una falta grave, no dar la adecuada protección y respaldo a los archivos críticos de la empresa. Para lograr la protección y optimización del uso conjuntamente con un esquema posterior de Contingencia *"Anexo 3 Figura 1"*contamos con los siguientes recursos:

- **Alternativas Electrónicas(Electronic Voulting)** se define como la posibilidad de guardar respaldos y obtener información de la misma en caso de necesidad, utilizando para ello la electrónica que permite intercomunicar el equipo donde se procesa la información con el centro de respaldo, esta conexión se hace directamente cuando los equipos en referencia se encuentran cercanos, o utilizando redes de banda local o banda ancha, existiendo en el centro de respaldo para recibir la información uno o varios de los siguientes equipos DASD, Mass Storage, librerías automáticas de cintas o discos(nearline)
- **Dasd** el costo de Dasd esta teniendo una efectiva tendencia a la baja, como consecuencia de ello, se esta almacenado un mayor volumen de información en línea, las nuevas tecnologías, hacen posible, que se incremente el almacenamiento de información estratégica de respaldo y de sistemas Non-Stop, en línea, además, podemos obtener imágenes especulares en áreas separadas. Estas tecnologías conocidas como RAID, permiten incluir al DASD como alternativas de respaldo. Esto puede lograrse al utilizar RAID 1, la solución más económica para el almacenamiento de contingencia en servidores non-Stop cuya necesidad de respaldo es de bajo volumen. La utilización de RAID 5, es más recomendable cuando el requerimiento es mantener imágenes de la información crítica de bases de datos de grandes dimensiones, que por sus características requieren operación constante (24x7x365) . Se debe acotar que, sin embargo, utilizar el DASD para almacenar gran volumen de información de respaldo sigue siendo comparativamente costoso, se debe minimizar la información a respaldar a la estrictamente necesaria.
- **Mass Storage** son equipos que utilizan técnicas de grabación en espiral similares a los de los casettes de video, capaces de grabar hasta 12 Gb en cintas de 4 u 8 mm. Un sistema simple compuesto por un servidor de control y 8 unidades de almacenamiento son capaces de almacenar 1.76 TB, en un área de aproximadamente 20 metros cuadrados. De acuerdo a lo estimado esto sería suficiente para almacenar una librería de 10000 tapes. Las unidades de Mass Storage son completamente automáticas en el proceso de captura y almacenamiento de la información y pueden recibir información por canales Fast SCSI llegando a movilizar hasta 20 GB/hora.
- **Librerías Automáticas de Cintas** como una variante especializada del concepto de Mass Storage surgió el de ATL(Automated Tape Library). El sistema ampliamente conocido, usa la robótica para seleccionar las cintas, cargarlas en la unidad y una vez concluida la acción, descargarla y retornarla a su posición original. El ATL, elimina por tanto la intervención humana, su uso es muy recomendando, para procedimientos de contingencia, bajo la figura de Electronic Voulting. *Su uso se justifica ya que*

las labores más exigentes en un ambiente de servidores centralizados, lo constituyen los procesos de impresión y respaldo que ocupan casi el 40% del tiempo de operación.

- **Discos Ópticos** uno de los continuos retos a los que nos enfrentamos en las operaciones de centros es buscar la manera más eficiente de guardar y acceder a la información. Frente a este reto se encuentra la necesidad de combinar el rápido acceso de la data tipo imagen y los problemas asociados con dicha información, aspectos en los cuales no han tenido éxito las tecnologías anteriormente mencionadas. La tecnología de discos ópticos permite guardar y acceder rápidamente la información y parece ser la tecnología que a mediano plazo se utilizará para acceder y respaldar la información "near line". La reusabilidad permite una alternativa operativamente comparable con los medios masivos de almacenamiento con mayor confiabilidad. Pero a pesar de los beneficios que esta tecnología proporciona su costo, es todavía , comparativamente alto, por tanto debe utilizarse conjuntamente con otros proyectos que le den valor agregado tales como distribución de imágenes, eliminación del papel y otros proyectos similares. *Entre los beneficios de esta tecnología cabe mencionar disponibilidad y accesibilidad de la información al ocurrir una interrupción, automatiza el proceso de recuperación en caso de desastre, es consistente con la meta de automatización y centralización de operaciones, mejora la disponibilidad de los procesos de respaldo y recuperación*
- **Hierarquical Storage Management (HSM)** es una tecnología que consiste en automatizar el balanceo del uso de los diferentes dispositivos antes mencionados y que conforman la pirámide de almacenamiento. Esta pirámide es la que se obtiene al ordenar en forma descendente las diferentes tecnologías de almacenamiento, desde la más cara(memoria de CACHE), hasta la más económica (cintas magnéticas). El HSM se implementa mediante software que se configura para que realice migraciones automáticas de data de un medio a otro de acuerdo a los parámetros definidos por el administrador.

Lineamientos Tecnológicos

- **RAID** si la tendencia en la cual nos movemos es hacia la centralización con plataformas distribuidas, con mejoras en los servicios a los clientes y operaciones 24x365, en un ambiente RDBMS (Relational Data Base Management System) para sistemas distribuidos y el sistema que sé esta implantando es OLTP(Online Transaction Processing) tendremos que pensar en esquemas con soluciones tipo non-Stop. En estos ambientes, debemos pensar en la protección, contar las fallas de discos como un primer esquema de respaldo, para ello ha emergido la tecnología RAID, ella nos permite producir imágenes estequiométricas de la información existente en los discos del sistema y ante una falla, en breve tiempo, se logra la recuperación y reconfiguración, que permite la continuidad de la operación. Dado los sistemas que se vienen utilizando en la institución, no se justifica el incremento desmesurado del espacio en disco para utilizar RAID 5, dado que los sistemas en línea tienen pocos días de requerimientos masivos y los mismos son predecibles(inscripciones, exámenes, nominas, etc)
- **Mass Storage** esta tecnología es la más popular para las operaciones de respaldo combinado con ATL se convierte en una solución completa de automatización del proceso de RR/AA. Presenta como problemas: una alta rata de errores en comparación con las tecnologías ópticas, sus exigencias de almacenamiento y una menor vida media. Pero su bajo costo y la facilidad de implantación la hace atractiva, *por lo que lo consideramos el más conveniente para procesos de Respaldo y Recuperación operacional*
- **Disco Optico** la necesidad de grabar información en imágenes**,** su preservación y mantenimiento, buscó una tecnología que permitiera economizar espacio que diera mayor velocidad de acceso y grabación cuya disponibilidad fuera expedita y más fácil de transportar. Si a lo referido anteriormente, agregamos que estos elementos continúan en la línea de automatización de operaciones y por tanto elimina la intervención humana en su proceso y mejorar la disponibilidad de respaldos, tendremos uno de los medios más idóneos para el proceso de respaldo de la información. Sin embargo en una comparación de costos con respecto a la tecnología de cinta mantiene una proporción de 5 a 2, pero con clara tendencia a la baja. Su utilización es recomendable si le damos valores agregados como sería la distribución de requerimientos que se hacen a los Centros de Información y algunos otros sistemas que requieren procesamiento de imágenes. *Se presenta como una tendencia que debe ser tomada en cuenta a mediano plazo para los procesos RR/AA*
- **HSM** la utilización de esta tecnología es vital para reducir los costos de operación de los servidores de la plataforma distribuida. Permite movilizar data poco referenciada de equipos sofisticados y caros

como RAID DASD, hacia equipos menos costosos como Discos Ópticos o Mass Storage, de forma automática y confiable.

Estrategia de Implantación dado que la RR/AA es un proceso de infraestructura crítica ya que afecta la disponibilidad y confiabilidad de la información. Debe ser prioritaria la implantación y automatización del proceso y para los efectos del plan consideró dos etapas:

- **Respaldo y Recuperación** dentro del esquema concebido en esta primera fase consideró como principal objetivo lograr un esquema de respaldo y recuperación que permita la operación con un amplio grado de confianza y para lograrlo parte de las siguientes premisas:
    1. **Control centralizado por área** la existencia de centros de control por área supone una serie de mecanismos que permiten entre otras cosas el control de los procedimientos básicos de operación, entre ellos debemos destacar el de Respaldo y Recuperación, su realización será controlada desde ese punto
    2. **Crecimiento** los sistemas se han creado para ser manejados y mantenidos en ambientes distribuidos y el ancho de banda disponible no aconseja el llevar a cabo respaldos centralizados
    3. **Ventanas de Respaldo definidas por el Usuario** los procesos de respaldos de BD y de algunas aplicaciones requieren que su operación no sea continua lo que afecta directamente la disponibilidad por tanto las fechas y frecuencias de los respaldos deben ser determinadas y definidas por los usuarios
    4. **Existencia de Sistemas Non-Stop en Servidores pequeños** aplicaciones y sistemas que dan servicio a un número pequeño de usuarios con requerimiento bajo de disco(hasta 10 GB) con alta criticidad en operaciones departamentales
    5. **Redundancia en el Servidor(RAID)** son esquemas integrados en el sistema de almacenamiento del servidor, con control autónomo, con el objetivo de disminuir el "Down Time" proveniente de fallas mecánicas o electrónicas
    6. **Respaldos distribuidos/Control centralizado** para aquellos servidores con una gran cantidad de datos a respaldar ubicados en localidades donde el ancho de banda no permita cumplir con las ventanas definidas por los usuarios
- **Administración de Almacenamiento** la implantación de esta etapa puede ser entendida como una extensión de la de respaldo y recuperación por lo que aplican las mismas premisas expuestas. se trata de optimizar la pirámide de dispositivos de almacenamiento en los que reside la información. Aquí lo básico es implantar un esquema HSM que optimice el uso de los recursos, facilite la planificación de la capacidad y en general coloque los datos donde sean requerido al momento que son necesitados, cumpliendo con ello el objetivo de seguridad. Para ello debemos:
    1. **Tipificar la información** según los criterios de administración que se deben definir con los usuarios, y personal de mantenimiento de sistemas. Los criterios que pueden ser utilizados son entre otros velocidad de respuesta, variabilidad, petición, etc
    2. **Definir Políticas de Migración** de la data en aquellos servidores que manejan grandes volúmenes de datos (más de 100GB) en los servidores centrales de los ambientes descentralizados
    3. **Utilización de Equipos que automaticen la operación** de acuerdo a las necesidades observadas por el costo y el tipo de información, el equipo en cuestión manejara la información en cinta
    4. **Control Autónomo** el proceso debe ocurrir sin intervención sólo se requerirán herramientas para generar estadísticas que permitan efectuar análisis de tendencias del uso de los recursos y detecten fallas que pudieran ocurrir en los procesos de respaldo

Impacto en Otras Infraestructuras los procesos RR/AA se conciben en forma batch, que deben llevarse a cabo en horas de poco uso de la red, a fin de beneficiarse del ancho de banda disponible. Por tanto no debe afectar los procesos en línea que por lo general operan en horas diurnas. Existen sin embargo procesos de recuperación que ocurren en horas laborables que si se utilizan con alta frecuencia pueden afectar el tiempo de respuesta de toda la red. Estas recuperaciones son usualmente de pequeños volúmenes de información. Recuperaciones de grandes volúmenes de información deben ser consideradas como excepciones y su impacto en el servicio de otros sistemas alertado. Por otra parte, las mejoras en otras infraestructuras, caso

específico de las redes locales, afecta directamente la ejecución y rendimiento de los procesos RR/AA, por lo que deben evaluarse antes y después de cada cambio

Situación Actual la situación que hemos encontrado es la siguiente:

- No existe una organización única encargada de RR/AA
- En algunas áreas se tiene experiencia en esquemas de respaldos
- No se observaron de manera general políticas ni documentación que apoye los esquemas de respaldo y contingencia en plataformas abiertas
- La operación que se lleva a cabo es manual, con débiles controles y en muchos casos inexistentes

Establecimiento de Proyectos y Metas Físicas en el mercado existen una variedad de paquetes que pueden llevar a cabo los esquemas de respaldo y contingencia, una vez se establezcan las políticas que regulen estas funciones, los costos de los mismos tienen poca variación al nivel de software, pero no ocurre lo mismo al nivel de hardware donde las diferencias son grandes. Para la implantación de procesos de respaldos se seleccionaron las siguientes tecnologías.

- Para almacenamiento en servidores con una sola unidad de menos de 10 GB soportando aplicaciones "non-Stop" utilizaremos tecnología de RAID
- Para respaldos generales estructuras de *Mass Storage 8 mm Exabyte con robótica*. Se debe evaluar el uso de disco óptico, en caso de variaciones importantes en el costo de las mismas.
- En proyectos que manejen imágenes, eliminación del papel, Centros de Correspondencia, GIS y como repositorio Nearline en un esquema HSM, se utilizara el disco óptico con robótica

Con relación al software se han analizado una serie de productos tomando en cuenta su funcionalidad, se ha determinado que para efectos de respaldo, los siguientes productos cumplen con la filosofía que se seguirá en los centros de control:

- *EMC/Epoch*
- *OMNIBACK*
- *ADSM*
- *Palindrome*
- *Netsys*
- *CommVault*
- *NearNet*

La diferencia de costos entre ellos no es sustancial, se basa en el pago de una licencia de uso y un pago por cada servidor a ser respaldada. En la selección debe buscarse por razones de economía y facilidad para la operación en la instalación que los productos puedan ser ubicados dentro del paraguas tecnológico que supone la infraestructura *"Tivoli" de IBM, "Openview" de HP, "Unicenter" de CA*

Proceso de Contingencia los esquemas observados no contemplan la estructuración de un Plan de Contingencia, razón por la que se recomienda la instauración de un plan, que arranque con un proceso de Business Impact Análisis a fin de determinar la importancia de los mismos para la empresa y los procesos vitales sobre los cuales aplicaría un esquema de contingencia.

De acuerdo a la infraestructura observada, recomendamos dos esquemas dependiendo del medio que se analice, para ello utilizaremos:

- **Para Servidores de Aplicación** se hará a nivel de área, su objetivo será que dado la desaparición física de un centro en la región, otro centro actuará como base de contingencia, utilizando los respaldos obtenidos y trabajando bajo un nivel de servicio menor motivado a la contingencia que se vive
- **Para Servidores de Base de datos** se centrara la contingencia en la sede central, utilizando tecnología de ADSM(Adstar Distributed Storage Manager) utiliza tecnología de LAN que nos proporciona Electronic Vaulting, es económico y automático

Plan de Respaldo Para Transacciones

Objetivo: Asegurar que en el transcurso del tiempo y partiendo de un respaldo válido y en buenas condiciones, podemos añadir las transacciones sometidas durante ese periodo y restaurar la base de datos dañada o corrompida.
Este procedimiento es básico para eliminar el riesgo de corrupción de información que pudiera derivarse por problemas diversos problemas, el mismo debe comenzar a aplicarse de inmediato y si bien se recomienda su permanencia en el tiempo. Si bien la recomendación es que este proceso se automatice, utilizando para ello un robot, y que se aplique además la tecnología de remote Vaulting, mientras esto no se lleve a cabo este procedimiento permanecerá activo

Responsable: Centro de Computación

Frecuencia: Diaria

Procedimiento:

Responsable	Actividad
Operador Centro de Computación	1. Al culminar las labores del día se debe correr el procedimiento de respaldo de transacciones, para ello tomará del rack de cintas la correspondiente al día que se va a realizar el respaldo. Las cintas estarán etiquetadas con el correspondiente día de la semana(Lunes, Martes....., Domingo) 2. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error 3. Si el proceso culmina de manera satisfactoria, almacenará la cinta en el rack correspondiente, e ira a paso 5 4. De presentarse algún error, determinará la causa, la corregirá e ira al paso 1 5. Si es Domingo, realizará el proceso de respaldo semanal; si es cualquier otro día de la semana, ir a paso 23 6. De ser Domingo; procederá a realizar el proceso de respaldo semanal, para ello, tomará del rack las cintas identificadas como(lunes,...,sábado) y las vaciará en una cinta identificada en el rack como (semana1,....Semana5), dependiendo de la semana del mes que se este procesando 7. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error, de terminar todo satisfactorio ir a paso 19 8. De presentarse algún error, determinará la causa, la corregirá e ira al paso 5 9. Si es el último día del mes, realizará el proceso de respaldo mensual; caso contrario ir a paso 23 10. Si es el último día del mes y no es Domingo, ir a paso 14

11. Es ultimo día del mes y domingo, si Ud. esta en este paso es porque el proceso diario y semanal han terminado satisfactoriamente, caso contrario ir a paso 13
12. Ir a paso 15
13. Es fin de mes y no es Domingo, proceda a correr un proceso semanal, con las cintas que comienzan en lunes y culminan con el día de la semana que esta procesando
14. Es fin de mes y no domingo; Procederá a realizar un proceso de respaldo semanal (extraordinario), para ello, tomará del rack las cintas identificadas como(lunes,...,sábado) y vaciará en una cinta identificada en el rack como (semana extraordinaria), las cintas correspondientes que deben empezar en lunes y culminar en el día de la semana que se esta procesando.
15. Vaciará todas las cintas semanales en una mensual
16. En el rack de cintas tome las correspondientes a las semanas y vacíelas en las correspondiente al mes que se esta procesando (Enero,...., Diciembre)
17. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error
18. De presentarse algún error, determinará la causa, la corregirá e ira al paso 11
19. Realizar una copia extra de la Cinta Semanal y/o mensual
20. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error
21. De presentarse algún error, determinará la causa, la corregirá e ira al paso 19
22. Traslade esta cinta a la Bóveda
23. Fin del Procedimiento

Plan de Respaldo Disco(Full Back up)

Objetivo: Asegurar la supervivencia de la información y sistemas del Centro de Computación de la institución. El mismo nos permite operar desde un centro de respaldo, en caso de una contingencia mayor

Responsable: Centro de Computación

Frecuencia: Semanal

Procedimiento:

Responsable	Actividad
Operador Centro de Computación	1. Para este proceso se requieren 6 cintas etiquetadas como semana1,semana2,....,semana5, Mensual1,Mensual2. 2. Es ultimo día del mes?, No ir a paso XX, tomar cinta Mensual1 y después de completar los respaldos parciales que deben llevarse a cabo, deberá ejecutarse un respaldo completo del disco y todos sus componentes. 3. Ir a paso 5 4. Es fin de semana?. Tomar cinta identificada con el número de la semana correspondiente, después de completar los respaldos parciales que deben llevarse a cabo, deberá ejecutarse un respaldo completo del disco y todos sus componentes. 5. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error 6. Si el proceso culmina de manera satisfactoria, almacenará la cinta(semana x o mensual x) en la bóveda y traerá al centro la cinta correspondiente a la semana o mes anterior, estas cintas permanecerán en el centro mientras se completa el ciclo semanal o mensual, posteriormente se reutilizaran 7. De presentarse algún error, determinará la causa, la corregirá e ira al paso 1

Plan de Respaldo de Sistemas

Objetivo: Asegurar que en el transcurso del tiempo y partiendo de un respaldo válido y en buenas condiciones, podemos recuperar un sistema que presente daños. Este procedimiento es básico para eliminar el riesgo de corrupción de información que pudiera derivarse por problemas o recuperación de un sistema o archivo dañado, su ejecución es obligatoria y en caso de falla debe identificarse claramente la causa, repararse y ejecutarse de nuevo. Si bien la recomendación es que este proceso se automatice, utilizando para ello un robot, y que se aplique además la tecnología de remote Vaulting, mientras esto no se lleve a cabo este procedimiento permanecerá activo.

Responsable: Centro de Computación

Frecuencia: Diaria

Procedimiento:

Responsable	Actividad
Operador Centro de Computación	1. Al culminar las labores del día se debe correr el procedimiento de respaldo de transacciones, para ello tomará del rack de cintas la correspondiente al día que se va a realizar el respaldo. Las cintas estarán etiquetadas con el correspondiente día de la semana(Lunes cls, Lunes bo, Martes cls, Martes bo ....., Domingo cls, Domingo bo) 2. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error 3. Si el proceso culmina de manera satisfactoria, almacenará la cinta en el rack correspondiente., e ira a paso 5 4. De presentarse algún error, determinará la causa, la corregirá e ira al paso 1 5. Si es Domingo, realizará el proceso de respaldo semanal; si es cualquier otro día de la semana, ir a paso 23 6. De ser Domingo; procederá a realizar el proceso de respaldo semanal, para ello, tomará del rack las cintas identificadas como (Lunes cls, Lunes bo,...,Sábado cls, sábado bo) y las vaciará en una cinta identificada en el rack como (semana cls1, Semana bo1 ....Semana cls5, Semana bo5), dependiendo de la semana del mes que se este procesando 7. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error, de terminar todo satisfactorio ir a paso 19 8. De presentarse algún error, determinará la causa, la corregirá e ira al paso 5 9. Si es el último día del mes, realizará el proceso de respaldo mensual; caso contrario ir a paso 23

10. Si es el último día del mes y no es Domingo, ir a paso 14
11. Es ultimo día del mes y domingo, si Ud. esta en este paso es porque el proceso diario y semanal han terminado satisfactoriamente, caso contrario ir a paso 13
12. Ir a paso 15
13. Es fin de mes y no es Domingo, proceda a correr un proceso semanal, con las cintas que comienzan en lunes y culminan con el día de la semana que esta procesando
14. Es fin de mes y no domingo; procederá a realizar un proceso de respaldo semanal (extraordinario), para ello, tomará del rack las cintas identificadas como(lunes cls, lunes bo,...,sábado cls, sábado bo) y vaciará en una cinta identificada en el rack como (semana cls, semana bo extraordinaria), las cintas correspondientes que deben empezar en lunes y culminar en el día de la semana que se esta procesando.
15. Vaciará todas las cintas semanales en una mensual
16. En el rack de cintas tome las correspondientes a las semanas y vacíelas en las correspondiente al mes que se esta procesando (Enero cls, Enero bo,...., Diciembre cls, Diciembre bo)
17. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error
18. De presentarse algún error, determinará la causa, la corregirá e ira al paso 11
19. Realizar una copia extra de la Cinta Semanal y/o mensual
20. Al culminar el proceso revisará que el mismo haya culminado satisfactoriamente y que no presenta ningún error
21. De presentarse algún error, determinará la causa, la corregirá e ira al paso 19
22. Traslade esta cinta a la Bóveda
23. Fin del Procedimiento

Actualización del Plan de Contingencia

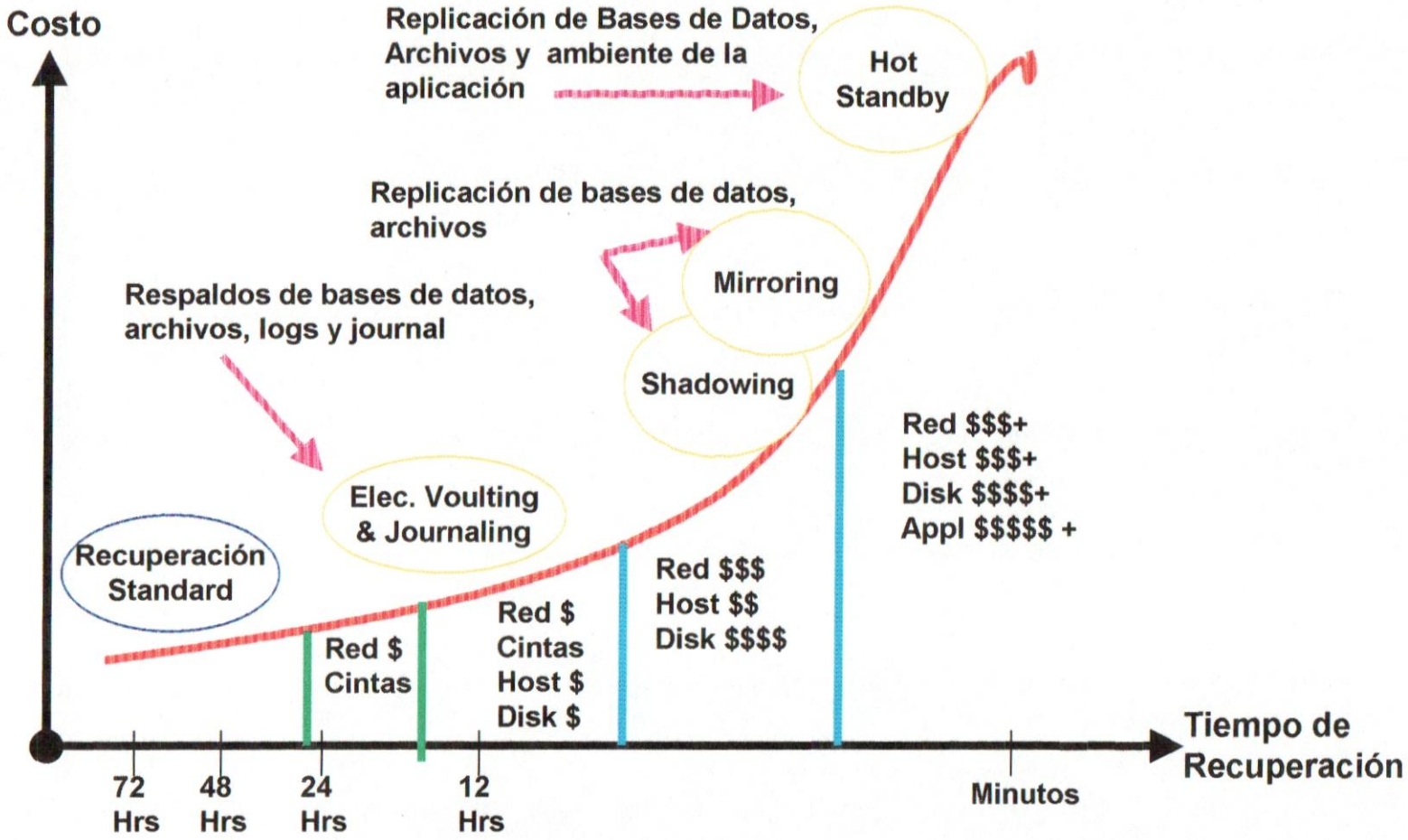
Objetivo: Si bien aun no existe un Plan de Contingencia en la institución, es necesario crear ciertos elementos que deben in en paralelo con el proyecto del plan de contingencia, básicamente estamos hablando de Control de Cambios.

Tal como se desprende del *"Anexo 3 Figura 1"* los diversos elementos que generan un cambio se originan de las siguientes vertientes:

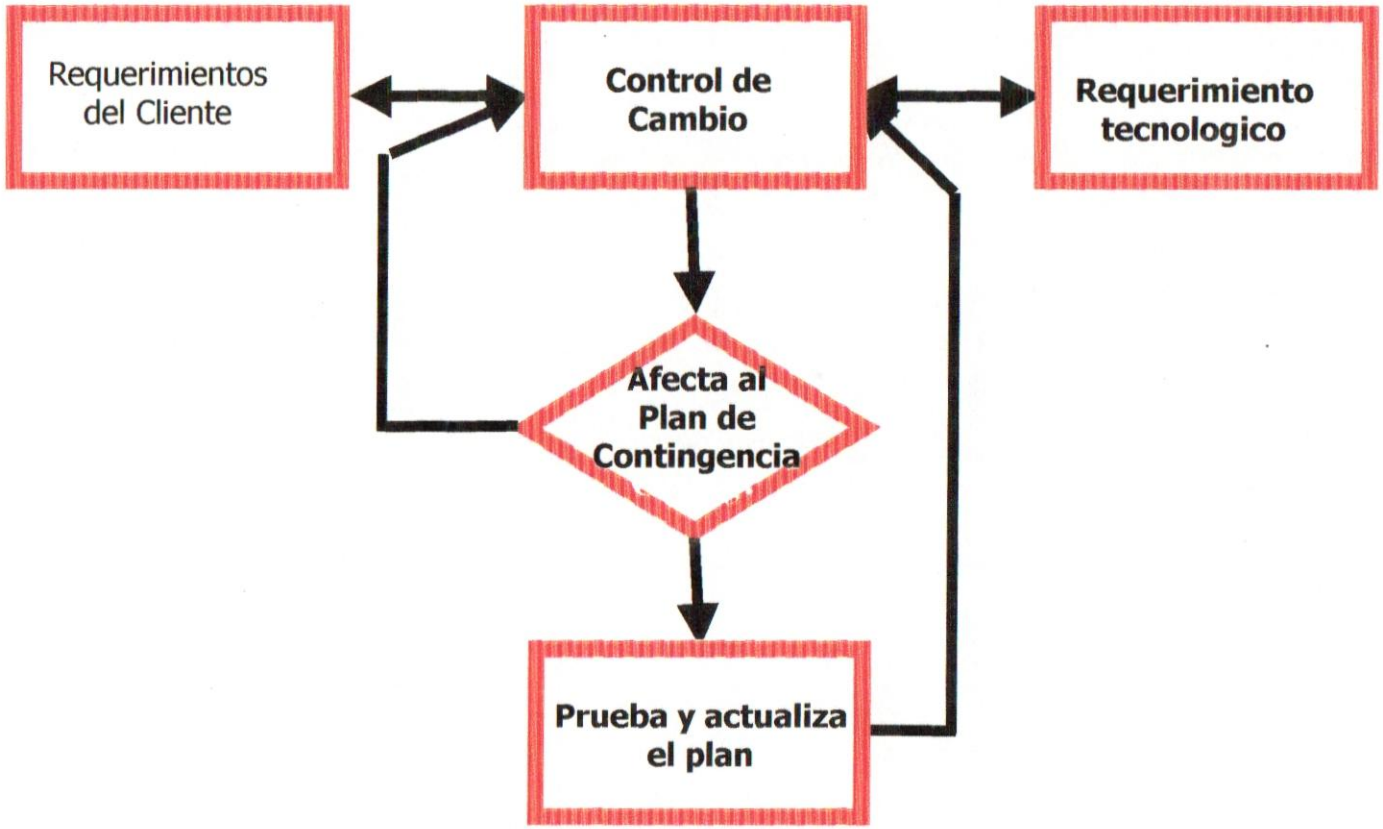
- Un problema detectado por un usuario y que requiere de un cambio en la red para ser solucionado
- Un cambio propuesto por el suplidor de servicio y que afecta de una forma u otra la continuidad del servicio
- Una falla detectada que requiere la interrupción de un servicio
- Una actualización al sistema operativo o de un software que se viene utilizando
- Un problema inesperado y que sin previo aviso afecta la continuidad del servicio

De acuerdo con este origen, procederemos a establecer el Control de Cambio, como un elemento proactivo que notifica al usuario sobre una problemática que afecta los niveles de servicio, además desde el punto de vista de continuidad el cambio puede afectar el Plan de Contingencia, por tanto cualquier cambio que afecte al Plan de Contingencia no puede ser considerado como un trabajo completado mientras no se actualice el Plan y se pruebe de manera fehaciente que la actualización del plan funciona perfectamente, si bien al final se requerirá de una herramienta que automatice este trabajo, pensamos introducir un procedimiento que cree la disciplina para finalmente implantarlo en todo su rigor

Disponibilidad y Costos



El Ciclo de Pruebas



Anexo 4

Auditoria de Laboratorios

1.1 Introducción La información es el patrimonio principal de toda institución, por lo cual es fundamental resguardarla y protegerla. Se deben aplicar medidas de seguridad para proteger la información y estar preparados para afrontar contingencias y desastres de diversos tipos. Las medidas de seguridad informática deben considerarse como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución. Como caso de estudio tomamos el Laboratorio de Seguridad Computacional, ubicado en la planta baja del edificio de laboratorios de Ingeniería, en este anexo haremos constante referencia a este laboratorio específicamente, hacemos constar que el modelo utilizado es ficticio, pero aplica y funciona.

- ✓ En el presente trabajo describiremos:
- ✓ La auditoria realizada al laboratorio de estudio.
- ✓ El Plan de contingencia propuesto.
- ✓ El Plan de penetración a seguir.
- ✓ Políticas de respaldo de información propuestas, con la finalidad de mantener la data segura y recuperable en caso de una contingencia.

A continuación se exponen una serie de conceptos que son necesarios para crear un contexto teórico que permita una mejor comprensión de las medidas y soluciones que serán planteadas.

1.2 Estrategia de Respaldo y Recuperación El presente documento tiene por objeto establecer las medidas de índole técnica y organizativa necesaria para garantizar la seguridad que deben reunir los archivos, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos.

1.3 **Definiciones**. A continuación se muestran una serie de definiciones necesarias para tener una mejor comprensión de las estrategias de respaldo y recuperación:

- **Sistema de información**: Conjunto de archivos, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- **Usuario**: Sujeto autorizado para acceder a datos o recursos.
- **Recurso**: Cualquier parte componente de un sistema de información.
- **Accesos autorizados**: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
- **Identificación**: Procedimiento de reconocimiento de la identidad de un usuario.
- **Autenticación**: Procedimiento de comprobación de la identidad de un usuario.
- **Control de acceso**: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- **Contraseña**: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
- **Incidencia**: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- **Soporte**: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.
- **Responsable de seguridad**: Persona o personas a los que se les ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- **Copia del respaldo**: Copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.

1.4 Objetivos:

- Proveer al Laboratorio de Seguridad Computacional un método estable y seguro para salvaguardar la información electrónica.

- Proveer un medio de protección que permita recuperar la información en un tiempo razonablemente corto de acuerdo a las necesidades de las aplicaciones.
- Contar con redundancia suficiente para permitir la recuperación en caso de dispositivos de almacenamiento externo (cintas) dañados en los respaldos.
- Proveer los medios de control necesarios para asegurarla corrección de errores de procesos a tiempo.

1.5 Metas:

- Realizar operaciones de respaldo, en base a las políticas de respaldo y recuperación que a continuación especificaremos, para proteger la información de cada día de trabajo.
- Respaldar todos los datos de usuarios o los cambios a los mismos.
- Permitir un medio flexible de respaldo.
- Respaldar la configuración del sistema y los archivos de seguridad en bases semanales.

1.6 Respaldo Jerárquico Es un aspecto crítico para asegurar protección a gran escala y a través del tiempo. La metodología general de respaldo se basa en el uso de jerarquías acumulativas y recurrencia. El respaldo se deberá efectuar en forma incremental de modo de respaldar periódicamente datos y aplicaciones, esto es ilustrado en los siguientes puntos. Para llevar a cabo este proceso se requiere apoyarse en un calendario anual de respaldos programados.

1.7 Jerarquía de respaldos del servidor del Laboratorio de Seguridad Computacional

- *Respaldo Trimestral:* efectuado cada 3 meses un respaldo completo de todo el sistema y sus aplicaciones. La rotación se efectúa en dos juegos de cintas.
- *Respaldo Mensual: mensualmente* se lleva a cabo un respaldo de sistema operativo, de las aplicaciones y las carpetas, se efectúa un respaldo completo de todo el sistema servidor y de las pc's instaladas en el usuario. Esto es con el propósito de evitar respaldos semanales redundantes al mensual. Regularmente estos respaldos se efectúan los lunes por la noche.
- *Respaldo Semanal:* este respaldo incluye todas las aplicaciones, datos y carpetas de usuario (No del sistema Operativo), también se respalda la seguridad del sistema y la configuración.
- *Respaldo Diario:* es un respaldo incremental en el que se salvan los cambios en las carpetas y las transacciones realizadas en el día.

Consideraciones de Excepción: todos los respaldos mencionados que ocurran en feriados planeados se llevan a cabo en el día exactamente anterior al feriado. Para feriados no planeados el respaldo se efectuará en el día próximo laboral

2 Políticas de Respaldo y Recuperación

2.1 Generales: Los procedimientos y estándares de respaldo y recuperación estarán regidos por el presente documento.

- Deberán existir respaldos en el almacén de cintas del laboratorio e iguales copias en localidades secundarias ubicadas fuera de la sede del laboratorio. Como sede secundaria, externa al edifico de laboratorios, se propone que se habilite un espacio dentro del, Centro de Aplicaciones Informática (CAI), dicho espacio se debe utilizar como almacén de copias de cintas de respaldo de los datos del Laboratorio de Seguridad Computacional.
- Deberá existir un inventario actualizado de todos los medios de almacenamiento.
- Deberá existir un inventario de las cintas de respaldo, tanto en el almacén del laboratorio, como en el almacén de copias de cintas de respaldo. En este inventario se debe especificar la fecha del respaldo, jerarquía del mismo (trimestral, mensual, semanal o diario) y ubicación (sólo en el almacén del laboratorio o en ambos almacenes) para tener un control de los respaldo mas recientes y poder ubicar de manera rápida los mismos. Este inventario se debe actualizar cada vez que se realiza un respaldo.
- Se debe elaborar una bitácora de entrada y salida de los respaldos que se mantienen dentro y fuera del laboratorio.
- En el centro de almacenamiento externo se debe contar con un acceso restringido del personal.

- La documentación de la estrategia de respaldo y recuperación deberá existir en forma escrita y en dispositivos electrónicos.
- Adquirir un medio de transportación donde se protejan las cintas de golpes, agua, magnetismos u otros elementos que puedan deteriorarlas.

2.2 Medio Operacional del Laboratorio de Seguridad Computacional:

- El acceso al laboratorio debe ser restringido.
- Todos los medios de almacenamiento externo deberán permanecer en el almacén de cintas.
- Todas las herramientas y equipo no utilizado deben permanecer en una bodega.
- No puede permanecer en el laboratorio ningún objeto que produzca magnetismo, debido a que estos objetos deterioran los equipos, así como las cintas de almacenamiento que se utilizan para realizar los respaldos.

2.3Traslado de Medios de Almacenamiento fuera de la Compañía

- Todo traslado debe ser autorizado.
- El traslado de los medios debe ser en un maletín con llave.
- El traslado lo debe realizar el operador de turno.
- Debe extender un recibo en cada localidad de respaldo.
- Debe existir un listado de personal autorizado en cada localidad de respaldo.

2.4 Esquema de rotación de cintas. A continuación se muestra el esquema de rotación de las cintas donde se va a realizar el respaldo de la información del Laboratorio de Seguridad Computacional.

- En las cintas **Cinta_L_i, Cinta_M_i, Cinta_Mi_i, Cinta_J_i** se realizará el respaldo diario de los datos, de acuerdo a la semana del mes.

- En las cintas **Cinta_V_i**, se realizarán los respaldos correspondientes a la semana i del mes actual.

- En las cintas **Cinta_Mes_i**, se realizará el respaldo mensual.

- Finalmente en las cintas **Cinta_Tri_i** se realizarán los respaldos trimestrales.

- Al final de un período de una año, se verá si las cintas se encuentran en buen estado para seguir siendo utilizadas, de lo contrario se hará la adquisición de un nuevo juego completo de cintas.

	Lunes	Martes	Miércoles	Jueves	Viernes	Mensual	Trimestral
1	Cinta_L_1	Cinta_M_1	Cinta_Mi_1	Cinta_J_1	Cinta_V_1		
2	Cinta_L_2	Cinta_M_2	Cinta_Mi_2	Cinta_J_2	Cinta_V_2		
3	Cinta_L_3	Cinta_M_3	Cinta_Mi_3	Cinta_J_3	Cinta_V_3		
4	Cinta_L_4	Cinta_M_4	Cinta_Mi_4	Cinta_J_4	Cinta_V_4	Cinta_Mes_1	
1	Cinta_L_1	Cinta_M_1	Cinta_Mi_1	Cinta_J_1	Cinta_V_1		
2	Cinta_L_2	Cinta_M_2	Cinta_Mi_2	Cinta_J_2	Cinta_V_2		
3	Cinta_L_3	Cinta_M_3	Cinta_Mi_3	Cinta_J_3	Cinta_V_3		
4	Cinta_L_4	Cinta_M_4	Cinta_Mi_4	Cinta_J_4	Cinta_V_4	Cinta_Mes_2	
1	Cinta_L_1	Cinta_M_1	Cinta_Mi_1	Cinta_J_1	Cinta_V_1		
2	Cinta_L_2	Cinta_M_2	Cinta_Mi_2	Cinta_J_2	Cinta_V_2		
3	Cinta_L_3	Cinta_M_3	Cinta_Mi_3	Cinta_J_3	Cinta_V_3		
4	Cinta_L_4	Cinta_M_4	Cinta_Mi_4	Cinta_J_4	Cinta_V_4	Cinta_Mes_3	Cinta_Tri_1

2.5 Traslado de las cintas. Una vez que haya finalizado una semana, se procederá a sacar del almacén de cintas, aquellas que correspondan con los días en específico de la semana, dejando únicamente la cinta que corresponde con el respaldo semanal.

Al finalizar un mes, se dejará en el almacén de cintas, solamente la que corresponda con el respaldo mensual, y se llevarán al almacén de copias de respaldo, aquellas cintas que correspondan con los respaldos semanales.
Al finalizar un trimestre, se procederá a trasladar las cintas correspondientes a los respaldos mensuales a al almacén externo, dejando en el almacén de cintas del Laboratorio, solamente la cinta que corresponde con el respaldo trimestral.
Una vez que haya finalizado un año, todas las cintas correspondientes a los respaldos trimestrales serán llevadas al almacén de copias de cintas de respaldo.
Cada vez que se realiza un traslado de algún respaldo, se debe actualizar en la bitácora, de entrada y salida de respaldos, el movimiento (del respaldo) del almacén del laboratorio hacia el almacén de copia de respaldo. En la bitácora del almacén del laboratorio se debe registrar: la fecha de salida del respaldo y el ID del respaldo. De igual manera se debe registrar en la bitácora del almacén de copia de respaldo: la fecha de entrada del respaldo y el ID del respaldo ingresado.

2.6 Procedimiento de restauración/Recuperación de la Información Cuando sea necesario obtener la información de respaldo almacenada en dispositivos de almacenamiento externo (cartucho, carretes, cintas, etc.) ya sea por ser restaurada temporalmente o para su recuperación, se procederá a localizar la cinta de acuerdo a la fecha de la cual se quiere obtener el respaldo. Esta localización se realizará consultando el inventario de respaldo que debe existir tanto en el almacén de respaldos dentro del laboratorio, como en el almacén de copias de respaldo ubicado en la sede externa al mismo. Una vez ubicado el dispositivo donde se almacena el respaldo, el operador de turno debe incorporar la cinta en el equipo y rescribir o sustituir la información existente por la información que se encuentra almacenada en la cinta de respaldo. En caso de que no se encuentre ninguna información en la computadora debe ingresar la información que se encuentra en el dispositivo de respaldo. Plan de Contingencia

2.7 Plan de Contingencia A continuación se muestra el plan de contingencia que se propone para el laboratorio de Circuitos Electrónicos y Redes
2.7.1 Jerarquización de las prioridades En primer lugar, para la definición del plan de contingencia, se procedió a asignar prioridades a cada uno de los sistemas y programas que se encuentran en el laboratorio, a continuación se muestra una tabla que contiene cada uno de los sistemas identificados dentro del laboratorio, así como la prioridad que le fue asignada de acuerdo a su grado de importancia y necesidad dentro del laboratorio.

Las prioridades fueron divididas en tres grupos:

- *Prioridad 1*: sistema necesario para el funcionamiento mínimo del laboratorio
- *Prioridad 2*: sistema importante dentro del laboratorio, pero se puede trabajar sin él por un algún tiempo.
- *Prioridad 3*: sistema cuya importancia dentro del laboratorio es poca, y se puede trabajar sin él por un período de tiempo largo.

Sistema	Prioridad	Observaciones
Sistema operativo Linux	Prioridad 2	Se puede laborar sin este sistema, ya que también se encuentra instalado el sistema operativo Windows en las máquinas.
Sistema operativo Windows	Prioridad 2	Se puede laborar sin este sistema, ya que también se encuentra instalado el sistema operativo Linux en las máquinas.
Lenguaje C (Windows)	Prioridad 3	Esta es una herramienta usada por los alumnos para las prácticas, pero se puede trabajar también en Linux con ella.
Servidor de correo (implantado para este trabajo por el grupo 1)	Prioridad 2	Este servidor de correo, aplicación de 2, no es de vital importancia

Archivos de trabajo (implantado para este trabajo)	Prioridad 1	Para el laboratorio los archivos creados para este trabajo son de mucha importancia para la clínica, por ello se les asigna esa prioridad.
Servidor Web Seguro (implantado para este trabajo)	Prioridad 2	Para el laboratorio no es de vital importancia el funcionamiento del servidor Web, por eso se le asigna esta prioridad.
Programa de encriptamiento (implantado para este trabajo1)	Prioridad 1	Este programa es muy importante porque es necesario para poder desencriptar los archivos de trabajo

2.7.2 Análisis de impacto Una vez que se han establecido las prioridades de cada uno de los sistemas, se procedió a efectuar un análisis de impacto, en este punto, se identificaron las posibles fallas que pueden ocurrir en el laboratorio, a cada una de ellas se le asigno un grado de impacto.
Los grados de impacto definidos para este análisis fueron:

- *Grado 1*: Las fallas correspondientes a este grado ocasionan la interrupción absoluta del funcionamiento del laboratorio
- *Grado 2*: Las fallas correspondientes a este grado producen graves daños a la productividad del laboratorio *Grado 3*: Las fallas correspondientes a este grado no producen daños a la productividad de los procesos que se llevan a cabo en el laboratorio.

Fallas posibles	**Impacto**	**Observaciones**
Destrucción completa o parcial de los archivos de la clínica	Grado 2	Esta información es crítica para el funcionamiento del laboratorio, pero deben existir respaldos de la misma que permitan seguir operando en un tiempo determinado.
Falla del servicio de correo interno (Software)	Grado 3	En caso de interrupción del servicio de correo electrónico, se puede seguir laborando sin mayor tipo de inconvenientes
Falla del servidor Web (Software)	Grado 3	En caso de interrupción del servicio de internet, se puede seguir laborando sin mayor tipo de inconvenientes
Falla de hardware del servidor (esta máquina contiene el servidor de correo, el servidor Web y la información de la clínica, el Firewall tipo Proxy y el antivirus)	Grado 1	Si se presenta una falla de hardware en esta máquina, es muy importante recuperarla, ya que contiene los archivos del laboratorio y los servicios que ofrece el centro de informática.
Falla de las máquinas cliente (Hardware)	Grado 3	Si se presenta una falla en alguna de las máquinas que se encuentran dentro del laboratorio, se puede utilizar cualquiera de las otras, ya que todas tienen exactamente la misma configuración.
Incendio completo o parcial del laboratorio	Grado 1	Si se presenta esta falla, el funcionamiento del laboratorio se verá interrumpido indefinidamente.
Inundación completa o parcial de la clínica	Grado 1	Si se presenta esta falla, el funcionamiento del laboratorio se verá interrumpido dependiendo de la magnitud del incidente.

Terremoto	Grado 1	Si se presenta esta falla, el funcionamiento del laboratorio pudiera verse interrumpido dependiendo de la magnitud del incidente.

2.7.3 Estrategias de solución ante las fallas A continuación se presentan las tareas y responsabilidades que deben ser tomadas en caso de que alguna de las fallas presentadas en la tabla anterior ocurra.

Destrucción completa o parcial de los archivos de la clínica			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Localizar el disco zip que contiene los últimos respaldos.	xxxxxxxx	15 minutos	yyyyyyyy
Restaurar los archivos en la máquina	xxxxxxxx	1 hora	yyyyyyyy
En caso de falla de las tareas anteriores			
No está el encargado	**No se halla el zip**	**Falla la restauración**	
El responsable debe asignar a un nuevo encargado que lleve a cabo las tareas anteriores.	Localizar un zip con respaldos anteriores	Identificar la falla y reemplazar el dispositivo dañado	

Falla del servicio de correo interno (Software)			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Verificar la integridad de la base de datos del correo y corregir inconsistencias	Administrador del servicio de correo	2 horas	Gerente de sistemas
Revisar y corregir los archivos de configuración	Administrador del servicio de correo	1 hora	Gerente de sistemas
Revisar los problemas de memoria y / o espacio en disco que pudieran haber ocasionado la falla	Encargado del SO	30 minutos	Gerente de sistemas
Levantar el servicio	Administrador del servicio de correo	1 hora	Gerente de sistemas
En caso de falla de las tareas anteriores			
Pérdida total de la BD	**Insuficiente memoria y/o espacio en disco**	Imposibilidad de levantar el servicio	
Localizar el respaldo más reciente y reponer la BD.	Sustituir o añadir el hardware necesario para incrementar el recurso insuficiente.	Hacer respaldo de la data existente y reinstalar el servidor de correo.	

Falla del servidor WEB (Software)			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Reiniciar el equipo	Administrador del servicio Web	15 minutos	Gerente de sistemas
En caso de falla de las tareas anteriores			
Persiste la falla		Imposibilidad de levantar el servicio Web	
Entrar a los archivos de configuración y hacer los ajustes necesarios		Reinstalar el servidor Web.	

Falla de hardware del servidor			
Tarea	**Encargado**	**Tiempo**	**Responsable**

Identificar el dispositivo que presento la falla	Técnico encargado del laboratorio	1 hora	CAI
Hacer el reemplazo del dispositivo y su respectiva configuración	Técnico encargado del laboratorio	2 horas	CAI
Restablecer la data en caso de que el dispositivo defectuoso sea un disco	Administrador del laboratorio	1 hora	CAI
En caso de falla de las tareas anteriores			
No se consigue el dispositivo de repuesto	Falla en el restablecimiento de la información		
En lo posible hacer uso de un dispositivo que cumpla con las funciones del defectuoso mientras se consigue el adecuado.	Verificar el nuevo dispositivo. De estar correcto, hacer uso de otro respaldo.		

Falla de las máquinas cliente (Hardware)			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Identificar el dispositivo que presento la falla	Técnico encargado del laboratorio	1 hora	CAI
Hacer el reemplazo del dispositivo y su respectiva configuración	Técnico encargado del laboratorio	2 horas	CAI
Restablecer la data en caso de que el dispositivo defectuoso sea un disco	Administrador del laboratorio	1 hora	CAI
En caso de falla de las tareas anteriores			
No se consigue el dispositivo de repuesto	Falla en el restablecimiento de la información		
En lo posible hacer uso de un dispositivo que cumpla con las funciones del defectuoso mientras se consigue el adecuado.	Verificar el nuevo dispositivo. De estar correcto, hacer uso de otro respaldo.		

Incendio completo o parcial del laboratorio			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Limpiar el laboratorio	Personal de limpieza de la institución	1 día	Institución
Análisis de la situación del laboratorio después del siniestro.	Técnico encargado del laboratorio	1 día	CAI
Configurar una de las máquinas cliente como servidor Web y servidor de correo en caso de que el servidor haya sido afectado.	Administrador del laboratorio	5 horas	CAI
Realizar las tareas correspondientes a las fallas de hardware mencionadas anteriormente	-	-	-

Inundación completa o parcial del Laboratorio			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Limpiar el laboratorio	Personal de limpieza de la institución	1 día	Institución
Análisis de la situación del laboratorio después del siniestro.	Técnico encargado del laboratorio	1 día	CAI
Configurar una de las máquinas cliente como servidor Web y servidor de correo en caso de que el servidor haya sido afectado.	Administrador del laboratorio	5 horas	CAI
Realizar las tareas correspondientes a las fallas de hardware mencionadas anteriormente	-	-	-

Terremoto			
Tarea	**Encargado**	**Tiempo**	**Responsable**
Limpiar el laboratorio	Personal de limpieza de la Institución	1 día	Institución
Análisis de la situación del laboratorio después del siniestro.	Técnico encargado del laboratorio	1 día	CAI
Configurar una de las máquinas cliente como servidor WEB y servidor de correo en caso de que el servidor haya sido afectado.	Administrador del laboratorio	5 horas	CAI
Realizar las tareas correspondientes a las fallas de hardware mencionadas anteriormente	-	-	-

3. Plan de penetración

3.1 Introducción Con el fin de asegurar la integridad de los servicios y la seguridad de la Clínica XYZ, se ha preparado un plan de penetración, el cual permitirá poner a prueba los diferentes servicios instalados. Entre estos servicios se pueden mencionar:

- Servidor Web Apache (Seguro): se cuenta con un servidor de Apache, el cual sirve las páginas Web del laboratorio y cuenta con un certificado Verisign de empresa, que permite a los usuarios tener un acceso seguro a la red.
- PGP (Pretty Good Protocol): el servidor cuenta con una aplicación que realiza encriptamiento de archivos mediante el uso del protocolo PGP, el cual permite mantener la confidencialidad de los archivos privados mediante el algoritmo de clave pública PGP.
- Servidor de correo: se cuenta con un servidor de correo SMTP llamado Qmail, el cual provee del servicio de correo electrónico.
- Firewall tipo Proxy: se cuenta con un servicio de Firewall, instalado mediante el uso de la herramienta BullDog, que permite hacer un filtrado de paquetes y configurar las direcciones IP permitidas para acceder a ciertos servicios.

- Anti-virus: Adicionalmente, como es de esperarse, el servidor cuenta con un anti-virus que en el presente es McAfee y que protege al mismo de los ataques externos mediante virus.

Tomando en cuenta lo anterior se ha preparado un plan general de ataque al servidor que provee los servicios anteriormente mencionados, así como un plan específico a cada servicio. Dicho plan es mostrado a continuación.

3.1.1 Plan general de ataque: Debido a la conocidas debilidades del sistema operativo Linux, se intentarán las siguientes acciones:
Se procederá a entrar al sistema como un usuario común, con la propia cuenta de la empresa auditora y revisar la permisología de los archivos de configuración una vez localizado en el directorio raíz "/". Así, los archivos cuya permisología indique rwx rwx rwx o alguna otra combinación que permita escritura de "others" podrá ser fácilmente eliminado mediante el comando **rm.**
Al entrar al sistema como un usuario común, la ejecución del comando **sudo** permitirá tener un acceso visible a los archivos del sistema. Se procederá a intentar la eliminación de los archivos de configuración básicos de cada uno de los servicios para los cuales esto aplique, observando la caída o no de cada servicio.
Se procederá a entrar al sistema operativo en modo "single", esto permite fácilmente la entrada de un usuario cualquiera a la máquina como Root teniendo así un control total sobre la misma. Si el archivo "lilo.conf" está configurado correctamente, la entrada no será permitida.
Se procederá a aplicar el programa de cracking de passwords obtenido en http://www.users.dircon.co.uk/~crypto/, obteniendo así el archivo desencriptado de passwords del sistema, con lo cual se podrá realizar cualquier tipo de atrocidad.

3.1.2 Plan de ataque al servidor Web: Mediante los métodos de acceso nombrados en el plan general de ataque, se procederá a aplicar los comandos **"stop"** o **"restart",** que se encuentran dentro del directorio de apache, bajo **/bin/.**
Adicionalmente, se procederá a modificar los archivos de configuración del mismo, encontrados en el directorio **/conf/**.
Se procederá a la realización de una modificación en la página principal del home del laboratorio, que en caso de ser exitosa leerá Dicha modificación de realizará sobre el archivo de índice (index.htm ó default.htm) en el directorio **/htdocs/.**

3.1.3 Plan de ataque al encriptamiento PGP. Adicionalmente al mecanismo expuesto de ataque al archivo de passwords del sistema, se procederá a abrir los archivos que se encuentren encriptados con PGP. Para ello, se utilizará el mecanismo de fuerza bruta, usando el Brute Forcer Munga-Bunga, el cual ha sido descargado de http://www.astalavista.com y que genera passwords aleatorios para romper la clave del algoritmo.

3.1.4 Plan de ataque al servidor de correo Para ello, se procederá a inundar el servidor de mensajes con archivos adjuntos pesados, esto permitirá verificar las políticas de prioridad de manejo de mensajes, así como evaluar el desempeño del mismo. Se procederá a enviar mensajes con virus informáticos, lo cual permitirá evaluar la política de antivirus de los clientes y el servidor, verificando si el servidor deja pasar los mensajes, los rebota o los desinfecta.

3.1.5 Plan de ataque al Firewall tipo Proxy Se procederá a inundar el Firewall de mensajes para verificar su comportamiento y corroborar que las políticas de manejo estén bien configuradas, esto permitirá evaluar el desempeño. Se procederá a alterar los encabezados de los paquetes a nivel de IP, colocando en sus lugar IPs que sean válidos según la lista de control de accesos, esto permitirá verificar que el servidor cuente con IPsec o un mecanismo alterno de protección de encabezados.

3.1.6 Plan de ataque al antivirus Como es de suponerse, el plan de ataque usado en este caso, será la ejecución de los diferentes tipos de virus almacenados con este fin, en las máquinas del cliente, así como el servidor. Esto permitirá verificar la actualización del antivirus.
Lista de virus a utilizar:

- Hahaha, enanito sí pero con que pedazo!
- Melissa

- Emmanuel
- Groovy
- Arbol de Navidad
- W97
- Virus de java (.jar)
- NetBeui
- Etc...

Anexo 5

Seguridad Física

1 Tarjeta Inteligente Una Smart Card o Tarjeta Inteligente es un dispositivo que lleva incorporado un microchip interno o externamente, con el cual puede almacenar, modificar y procesar información. Hay toda una gama de tarjetas que caen dentro de la categoría de *Smart Card* y la mayoría de ellas se distinguen por la manera en que procesan la información, las capacidades del chip, así como también el tipo de contacto que traen.
El termino *Smart Card* es en sí muy ambiguo y es usado de diferentes maneras. Para la **ISO** *Smart Card* corresponde a lo que ella denomina **ICC** (Integrated Circuited Card) y envuelve a todos los dispositivos donde un circuito integrado cumple con los estándares impuestos para tarjetas plásticas de identificación **ID1**. La tarjeta es de 85.6*mm* *x* 53.98*mm* *x* 0.76*mm* y es igual a la tarjeta de cinta magnética que las entidades financieras emplean como instrumento de pago (tarjetas de crédito).

1.1 Arquitectura funcional las Smart Cards cuenta con una unidad de procesamiento central de 8 bits a 5 Mhz. Opcionalmente (dependiendo del tipo de fabricante) cuenta con un coprocesador. En cuanto a memoria puede tener cuatro tipos:
RAM: de 128 a 1024 bytes
ROM: de 4 a 64 Kbytes
EEPROM: 3 a 16 Kbytes
Flash
El tiempo promedio de lectura escritura es de 20 ms., si utiliza RSA Rivest-Shamir-Adleman (512 bits): 100 ms

1.2Tipos de Smart Cards a pesar de haber un estándar establecido por la **ISO** tanto para la manufacturación como para funcionalidades básicas que debiera incorporar una *Smart Card.* Existen dos tipos de clasificaciones. La primera de ellas tiene que ver con el tipo de chip que va en su interior, así como también la forma en que procesa la información. La otra manera de clasificarlas está relacionada con el tipo de contacto que tiene que tener la tarjeta para entrada y salida, así como también la fuente de poder.

- Caracterización por el tipo de Microchip
  - Smart Cards de Memoria
  - Smart Cards de Memoria con Lógica de Seguridad
  - Smart Cards Inteligentes
- Clasificación de Smart Cards por el Tipo de Contacto
  - Smart Cards de Lectores con Contacto
  - Smart Cards de Lectores sin Contacto
  - Smart Cards para Ambos Lectores

1.3 Estándares en Smart Cards como una manera de prevenir la proliferación de múltiples sistemas de *Smart Cards* se ha establecido estándares tanto en las funcionalidades mínimas que debiera tener una tarjeta, así como los protocolos y diseño. De esta manera la *ISO* fue la primera organización en establecer un modelo de *Smart Card.* A pesar de ello, hoy en día casi todas las tarjetas tienen aspectos en común pero eso no obliga a que un diseño en especial deba regirse por estos estándares.
El Estándar OpenCard es un estándar abierto que provee interoperabilidad de aplicaciones de *Smart Card* a través de **NC**s, **POS**s, desktop's, laptop's, etc. **OpenCard** promete proveer el 100 % de aplicaciones para *Smart Card* en *Java* puro. Las aplicaciones para *Smart Cards* a menudo no son puras debido a que ellas se comunican con un dispositivo externo y/o usan librerías en el cliente. OpenCard también provee desarrolladores con una Interface a **PC/SC** para el uso de los dispositivos existentes en plataformas de *Win32.* **OpenCard** para cumplir con las metas propuestas tomó los protocolos de los estándares. Básicamente la aplicación se comunica con el lector, el cual vuelve a comunicarse con la *Smart Card* usando un protocolo, que en este caso es el establecido en el **ISO 7816**. La idea de **OpenCard** es conectar la *Smart Card* con una aplicación de *Java.* Para ello tiene establecido un protocolo llamado **APDU** (Aplication Protocol Data Unit), el que puede ser considerado un paquete de datos que contiene una instrucción completa o una respuesta completa desde la tarjeta. Para proveer esta funcionalidad, **APDU**

tiene una estructura bien definida que esta inserta dentro de los documentos pertenecientes a la familia de especificaciones de la **ISO 7816**. La idea detrás de todo lo anterior es que a través de un dispositivo lector que se conecta a un PC, sería posible realizar transacciones seguras vía Internet, independiente de la plataforma donde esté conectada la tarjeta, gracias a *Java*.

1.4 Los Estándares de la ISO la *Smart Card* más básica que cumple los estándares es la de la serie **ISO 7816**, detalla la parte física, eléctrica, mecánica y la interfaz de programación para comunicarse con el microchip. La descripción de cada una de las partes de la **ISO 7816** es:

- IS 7816-1 (1987): Características Físicas.
- IS 7816-2 (1988): Dimensiones y ubicaciones de los contactos.
- IS 7816-3 (1989): Señales Electrónicas y Protocolo de Transmisión
- IS 7816-4 (1995): Respuestas y Comandos Ínter industrias.
- IS 7816-5 (1994): Sistema de Numeración y procedimiento de registro.
- IS 7816-6 (1996): Elementos de datos Ínter industrias.
- (DIS) 7816-7: Comandos Ínter industrias y Consultas Estructuradas para una Tarjeta
- (DIS) 7816-8: Comandos Ínter industrias Relacionados con Seguridad.
- (DIS) 7816-10: Señales electrónicas y Respuesta al *Reset* para una Smart Card Síncrona.
- Una descripción para las *Smart Cards* sin contacto está descrita en el estándar **ISO 14443**

1.5 Tipos de Protocolos de Comunicación hay dos protocolos de uso general que están en uso hoy en día: **El protocolo T=0** es un protocolo predominante en Francia y fue solamente un protocolo especificado en el documento **ISO 7816-3**.
Protocolo T=1 en 1992 la **ISO** estandarizó el protocolo T=1 como una corrección a el **ISO 7816-3**. Por supuesto que la **IC** y el dispositivo de Interface deben operar con el mismo protocolo. El método por el cual ellos alcanzan una óptima configuración en común ha sido el objeto de muchas discusiones al respecto en los últimos años. Al consenso que se ha llegado es tener una instrucción que seleccione el tipo de protocolo, esta instrucción es la llamada PTS (*Protocol Type Selection*). Hay efectivamente un comando especial que envía el dispositivo de interfase a la **IC** después de la respuesta al *reset*. Para mantener compatibilidad con sistemas comerciales que solamente pueden emplear el protocolo de comunicación T=0, algunos cambios son necesarios hacer en el estándar original de la **ISO 7816-3**. Un nuevo concepto está propuesto el cual identifica el principio de los dos modos de operación:
Modo Negociable Una **ICC** que opera en un modo negociable pueden cambiar su protocolo de comunicación por el uso del comando **PTS**. Una **ICC** que opera en el **modo específico** no puede aceptar un comando **PTS** pero puede ponerse dentro del modo negociable para una confirmación adicional del comando reset.
Aunque la **ICC** indica al dispositivo de internase su capacidad para cambiar al modo negociable, un dispositivo existente en el lado mercado puede sin embargo despreocuparse de aquellos cambios y por lo tanto no estar preparado para el reset de la tarjeta.

1.6 Utilidades:

- Almacén móvil de datos
- Dispositivos seguro
- Manejo sencillo

1.7 Utilización

- Identificación y autenticación
- Sistema de pago
- Transporte de datos
- Sistema criptográfico auditable y homologable

1.8 Vulnerabilidades

- Manipulación del dispositivo
- Ataques criptográficos
- Sondas electromagnéticas
- Ingeniería social

Anexo 6

Acceso al Medio

1.- Data Encryption Standard (DES) el esquema más extendido en encriptación de datos es el DES, que fue adoptado en 1977 por el National Institute of Standard and Technology (NIST), como el Federal Information Proccesing Standard 46 (FIPS PUB 46). Para el DES la data era encriptada en bloques de 64 bits utilizando una clave de 56 bits. El algoritmo transforma los 64 bits del bloque de entrada a través de una serie de pasos en un bloque de 64 bits de salida. Estos mismos pasos y utilizando la misma clave se utiliza para revertir la información. El DES si bien se ha extendido muy rápidamente, también ha sido fruto de muchas controversias, por lo que conviene revisar la historia del DES. A finales de los años 60 IBM liderizó un proyecto basado en criptografía computacional liderizado por Horst Feistel y que concluyó en 1971, con el desarrollo de un algoritmo conocido como LUCIFER(FEIS73), el cual fue vendido a Lloyd de Londres para ser usado en un sistema para dispensar dinero en efectivo que también fue desarrollado por IBM. LUCIFER era un bloque Cipher que operaba en bloques de 128 bits, con claves de 128 bits, en vista de los prometedores resultados obtenidos, IBM se embarco en un proyecto que le permitiera obtener un producto de encriptación que pudiera ser implantado en un chip sencillo. El esfuerzo fue liderizado por Walter Tuchman y Carl Meyer, incluía no sólo investigadores de IBM, además consultores externos y técnicos de NSA. Como resultado de este esfuerzo surge una versión refinada de LUCIFER, que reduce el tamaño de su clave original en 72 bits, alegando que la clave era muy corta y que en un ataque de "Fuerza Bruta" podría ser descubierta. El segundo elemento de crítica era la estructura interna que se consideró y todavía lo es información clasificada, por tanto no podemos determinar la debilidad que pudiera tener en su estructura interna, si bien trabajos posteriores indican que su robustez es lo suficientemente fuerte.

1.1 Encriptación DES el proceso de encriptación DES es mostrado en el *Anexo 6 Figura 1*. Existen dos entradas para la función de encriptación la formada por el Plaintext "A" y la otra "B" que utiliza la clave de encriptación. En el lado izquierdo de la figura podemos deducir que el proceso se lleva a cabo en tres etapas, en la primera el bloque de 64 bits pasa por una permutación inicial, que realiza un re-arreglo de los bits para producir un "Input permutado". Esto va seguido por una fase que consiste en 16 iteraciones de la misma función que envuelve un proceso de permutación y sustitución de la función. El output de las ultimas 16 iteraciones es una salida de 64 bits derivados de la información original en Plaintext y de la clave que se esta utilizando.
Los pasos que podemos observar a la izquierda y a la derecha se van sucediendo para producir un "Preoutput" y finalmente este es pasado a una permutación $\mathbf{IP^{-1}}$ que es la inversa de la función de permutación inicial dando como resultado un bloque de Ciphertext de 64 bits.
La porción derecha nos muestra como la clave de 56 bits es usada. Inicialmente la clave pasa por un proceso de permutación y posteriormente para cada una de las iteraciones se produce una clave $(\mathbf{K_j})$ es producida por la combinación y permutación que lleva a cabo el "Left Circular Shift". La función de permutación es la misma en cada iteración pero produce una subclave diferente.

2 Claves Públicas y Privadas el desarrollo de la clave pública es la más grande y posiblemente la única revolución en toda la historia de la criptografía. Desde el inicio de la criptografía a la actualidad los sistemas se han buscado unas herramientas elementales que lo que realizan son sustituciones y permutaciones. Después de miles de años haciendo estos cálculos a mano se logró un primer gran avance con la máquina Rotor de encriptación. Esta máquina electro mecánica permitió el uso de complejas técnicas de encriptación. Con la aparición del computador se avistaron esquemas mucho más complejos siendo el más prominente de ellos LUCIFER, desarrollado por IBM y que culminó con el DES. Pero si bien tanto Rotor como LUCIFER significaron grandes avances, continúan siendo herramientas que tienen como base combinaciones y permutaciones.
La criptografía de Clave Pública proporciona una abertura radical frente a todo lo que existía anteriormente, por una razón los algoritmos de clave pública están basados en funciones matemáticas en vez de simples combinaciones y permutaciones. Pero más importante que eso es el hecho de que la Clave Pública es asimétrica, lo que implica el uso de claves separadas en contraste con los mecanismos convencionales Simétricos de encriptación que sólo usan una clave. El uso de dos claves tiene profundas consecuencias en el área de la confidencialidad, la distribución de la clave y el proceso de autenticación.

2.1 Principios de Clave Pública el concepto de Clave Pública evoluciona a fin de atacar los principales problemas relacionados con la encriptación convencional, el primero relacionado con la distribución de las claves, que en un sistema convencional requiere:

1.- que dos entes que se estén comunicando compartan una clave la cual de alguna manera ha sido distribuida.

2.- El uso de un centro de distribución y esto con Diffie Hellman, descubridores del principio de Clave Pública elimina el principio de Criptografía que es mantener el secreto de la comunicación. Otro problema expuesto por Diffie tiene relación con las firmas digitales "Si el uso de la criptografía se extiende más allá de las situaciones militares y llega a las situaciones comerciales y para propósitos privados entonces los mensajes electrónicos y los documentos necesitan el equivalente a la firma que hacemos en papel. Por esto se desarrolló un método que estipula la satisfacción de ambas partes cuando un mensaje ha sido enviado a una persona en particular". Diffie y Hellman en 1976 dieron con un método que vendría a resolver los dos problemas que se presentaban

.

2.2 El Sistema de Clave Pública desde el punto de vista de los esquemas de encriptación de claves usadas para encriptar y desencriptar un mensaje determinado son las mismas. Esto no es una condición necesaria, en su lugar se hace posible desarrollar un algoritmo que deja en una clave para encriptar y una diferente pero relacionada con la anterior para desencriptar, además este algoritmo tendría las siguientes características:

- Que sea computacionalmente imposible determinar la clave de encriptación sólo con conocer el algoritmo y la clave de encriptación
- Cualquiera de las dos claves puede ser usada por el proceso de encriptación , mientras que la otra será usada para descifrar la información

Los pasos esenciales para lograr esto son:

1. Cada sistema final en una red generará un par de claves usadas para encriptar y descifrar los mensajes que se recibieran.
2. Cada sistema publica su clave de encriptación poniéndolo en un registro público o archivo, esto es lo que se conoce como la Clave Pública, manteniendo la segunda clave en privado
3. Si "A" desea enviar un mensaje a "B", "A" encripta la información utilizando la clave pública de "B"
4. Cuando "B" recibe el mensaje lo descifra utilizando su clave privada, ningún otro lo puede hacer pero sólo el conoce su clave privada.

Veamos ahora los elementos esenciales de un proceso de encriptación de Clave Pública.

Existe una fuente de información "A", para un mensaje en Plaintext, produciendo el mensaje $\mathbf{X= [x_1, x_{2,}, x_n]}$, en donde los N elementos de X son letras de un alfabeto finito. El mensaje tiene un destino que es "B". "B" ha generado un par de claves, una pública $\mathbf{K_{ub}}$ y una privada $\mathbf{K_{rb}}$, que es secreta y sólo conocida por "B", para "A" es accesible la clave pública de "B".

Con el mensaje y la clave de encriptación $\mathbf{K_{ub}}$ como entrada de A origina el Ciphertext $\mathbf{Y= [y_1,y_2,....,y_n]}$, por tanto $\mathbf{Y=E_{kub}(X)}$. B conoce su clave su clave privada y con ello puede invertir la función transformándola en $\mathbf{X=D_{Krb}(Y)}$

Un oponente observando Y, además con acceso a $\mathbf{K_{ub}}$ pero sin acceso ni a X ni a $\mathbf{K_{rb}}$, debe intentar conocer alguno de los dos factores anteriores, si además asumimos que el oponente conoce el algoritmo de cifrado y descifrado. Si esta sólo interesado en el mensaje en particular enfocara su trabajo sobre X, si esta interesado en leer todos los textos que se reciban se focalizará en $\mathbf{K_{rb}}$

Como mencionamos anteriormente cualquiera de las dos claves puede ser utilizada para encriptar mientras que la otra es para descifrar. Esto presenta un esquema de confidencialidad. Si bien el esquema anterior nos presenta un elemento importante de confidencialidad, busquemos ahora uno que nos presente autenticación y tendremos $\mathbf{Y=E_{Kra}(X);\ X=D_{Kua}(Y)}$

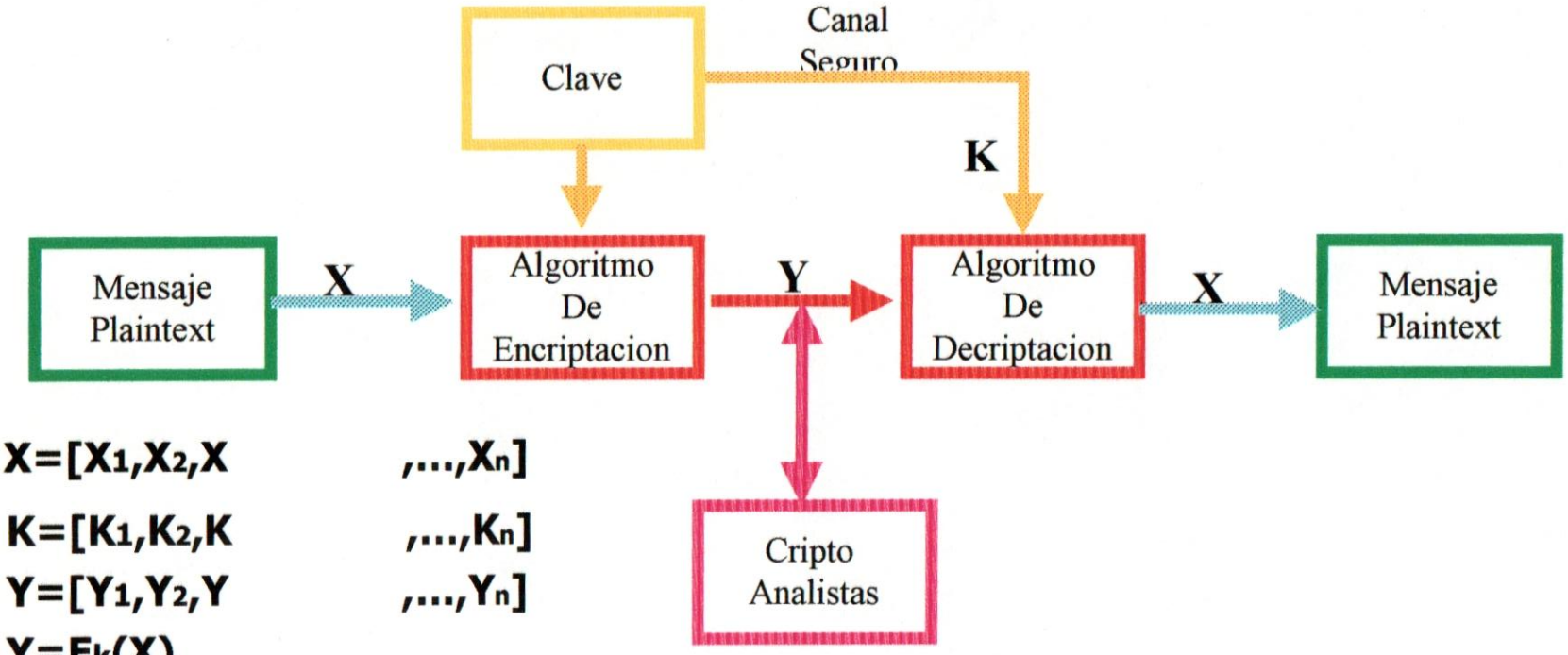
En este caso A prepara un mensaje para B y lo encripta usando la clave privada de A antes de transmitirlo, B utiliza la clave publica de A para descifrarlo. Dado que el mensaje se genero con la clave privada de A, solo el pudo enviarlo el propio mensaje sirve como firma digital, además la única forma de alterar el mensaje es accediendo a la clave privada de A, por tanto el mensaje es autenticado en términos de su fuente lo que asegura integridad. in embargo podemos crear un proceso adicional que permita tanto la confidencialidad y la autenticación, para ello utilizaremos un doble esquema de la Clave Pública

$\mathbf{Z=E_{kub}[E_{kra}(X)]}$

$\mathbf{X=D_{kua}[E_{krb}(Z)]}$

Figura 6.2

Algoritmo de Encriptación



$X=[X_1,X_2,X \quad ,\ldots,X_n]$

$K=[K_1,K_2,K \quad ,\ldots,K_n]$

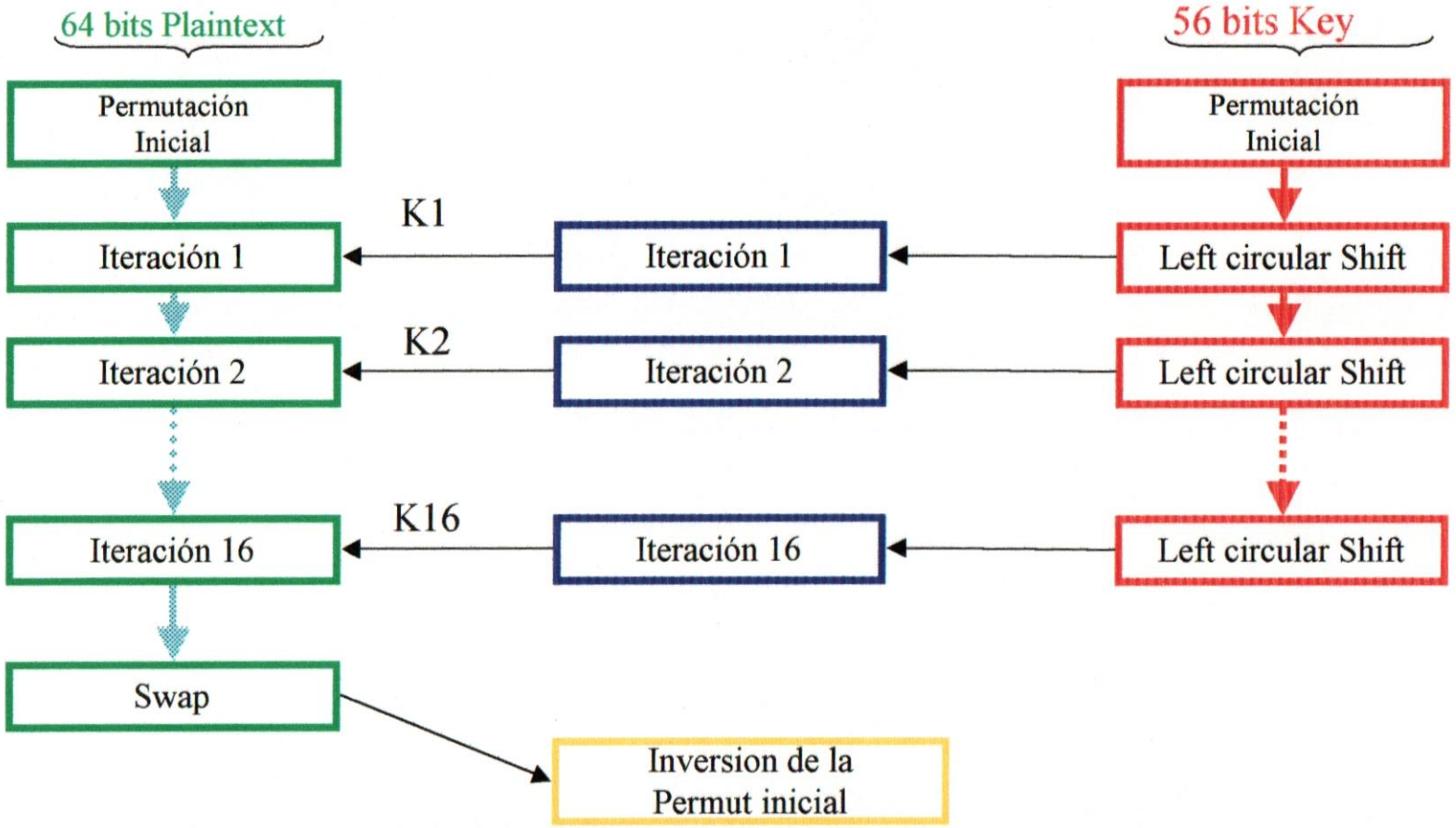
$Y=[Y_1,Y_2,Y \quad ,\ldots,Y_n]$

$Y=E_k(X)$

$X=D_k(Y)$

Anexo 6 Figura 1

Data Encription Standard(DES)



Comenzamos igual que en los dos casos anteriores, encriptando un mensaje usando la clave privada del remitente, lo que nos proporciona la firma digital e integridad, a continuación encriptamos nuevamente con la clave pública del receptor. El Ciphertext final sólo puede ser descifrado por la clave privada del receptor lo que nos asegura el principio de confidencialidad que se nos había requerido al principio del problema

2.3 Requerimientos para la Criptografía de Clave Pública todo lo anterior publicado esta basado en un algoritmo basado en dos claves relacionadas. Diffie y Hellman establecieron las bases para que esto funcione y es conocido como DIFF76B

- Es fácil para el receptor "B" generar una clave pública y una privada
- Es fácil para el remitente "A", conociendo la clave pública y el mensaje que sé encriptará "M" puede generar el Ciphertext $C=E_{kub}(M)$
- Es computacionalmente fácil para el receptor "B" descifrar el Ciphertext resultante usando la clave privada para recuperar el mensaje original $M=D_{krb}(C) = D_{krb}[E_{kub}(M)]$
- Es computacionalmente imposible para un oponente conociendo la Clave pública K_{ub} y el Ciphertext "C" recuperar el mensaje "M"

3 Secure Socket Layer (SSL) El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP. Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como *SSL Handshake*. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Tras finalizar la transacción se termina SSL.

3.1 Como trabaja SSL? *Solicitud de SSL:* Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio. Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el *SSL Handshake*. Durante el H*andshake* se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL. Los pasos que se siguen son los siguientes:

- Client Hello: El "saludo de cliente" tiene por objetivo informar al servidor que algoritmos de criptografía pueden utilizar y solicita una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define como cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.
- Server Hello: El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de que algoritmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.
- Aprobación del Cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el Handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

- Verificación: En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fue enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el Handshake se completa, de otra forma se reinicia el proceso.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El Handshake se realiza solo una vez y se utiliza una llave secreta por sesión.

3.2 Intercambio de datos*:* Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash de una vía acordado durante el Handshake), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

3.3 Terminación de una sesión SSL*:* Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

3.4 Implementación de SSL.- Como ya se ha comentado anteriormente, el sistema más utilizado en la actualidad para garantizar pagos seguros por Internet es el SSL (Secure Socket Layer), un protocolo de seguridad que se ha convertido en un estándar de Internet y que viene incluido por defecto en los navegadores Microsoft Explorer y Netscape Navigator. Lo que permite una implementación muy sencilla del sistema de pago ya que el cliente puede comenzar a comprar sin tener que realizar ningún proceso de autentificación previa. Los servidores seguros SSL los podremos notar porque en al esquina inferior izquierda cambia a una llave cerrada en el caso de Netscape. En la URL, cambia de Http:// a Https:// (Hypertext Transport Protocol Secure).

3.5 Deficiencias SSL fue creado como un protocolo de comunicaciones seguro de uso genérico, por tal razón presenta usa serie de deficiencias que deben tenerse en cuenta.

- *Confidencialidad:* SSL garantiza la confidencialidad extremo a extremo pero una vez finalizada la conexión, se poseen todos los datos y se estaría expuesto a cualquier tipo de fraude por parte de toda persona que tuviera acceso a dicha información.
- *Integridad:* SSL no garantiza la integridad de la información una vez finalizada la conexión, por lo que podría modificar esos datos para efectos de fraude.
- *Autentificación:* no necesita autentificarse, una persona con acceso a información, podría utilizarla para cometer fraude, es el más común delito y que causa mayores perdidas a las compañías de crédito.
- *No repudio:* no existe ningún tipo de comprobante por lo que cualquier protesta posterior carecerá de medios para su confirmación.

Con SSL, toda la seguridad recae en la confianza que entre las partes, ya que potencialmente se puede realizar cualquier tipo de fraude con total impunidad. SSL utiliza Certificados digitales siguiendo el estándar X.509, es decir, certificados de propósito general. Seria más interesante que existieran Autoridades Certificadoras creadas especialmente para emitir certificados de este tipo y que dichas Autoridades estuvieran avaladas por la banca de tal modo que los certificados digitales expedidos tuvieran conexión con cuentas de bancarias concretas. El rol de las autoridades certificadoras.- Además de asegurar el canal a través del cifrado, SSL de Netscape proporciona la autentificación del servidor. El AC endosará solamente la identidad del servidor Web. Esto significa que los usuarios finales pueden estar seguros de la identidad del Web site que están conectando, pero no hay seguridad de la calidad del contenido del Web. La inclusión de ACs en el software del Browser significa que los usuarios finales confían implícitamente en cualquiera de los sitios del Web certificados por éstas ACs. Los sitios establecen confianza construyendo las firmas públicas de las autoridades de la certificación en los browsers.

4 Protocolo SET.- Las empresas de crédito son las principales interesadas en que el uso de las Tarjetas de Crédito se generalice en todos los ámbitos de la vida, incluyendo evidentemente a Internet. No es de extrañar por tanto que las dos empresas más importantes de este sector, Visa y MasterCard uniesen

esfuerzos y potenciaran la creación de un nuevo protocolo que permita los pagos por Internet de un modo totalmente seguro, sin las limitaciones que plantea SSL. La idea básica consistía en crear un protocolo especialmente diseñado para garantizar la seguridad en el pago mediante Tarjetas de Crédito a través de medios de comunicación inseguros como es el caso de Internet y que este protocolo se convirtiese en un estándar abierto para la industria que sirviese de base a la expansión del Comercio Electrónico por Internet Para ello debían contar con el apoyo de las principales compañías informáticas, así que al proyecto se le unieron empresas de la talla de Microsoft, Netscape, IBM, Verifone-HP, GTE y contaron como desarrolladores a RSA Data Security, Verisign, Terisa-Spyrus y SAIC. El 31 de Mayo de 1997 se hicieron públicas las especificaciones formales del protocolo SET versión 1.0, estas especificaciones se pueden encontrar el Web oficial de SET, <www.setco.org>. Los documentos oficiales son:

- Book 1: Descripción de negocio
- Book 2: Guía para Programadores
- Book3: Descripción formal del protocolo
- Guía de interfase externo.- En este documento se dan las normas para la conexión por Internet, ya que SET internamente no especifica el tipo de protocolo de comunicación que debe utilizarse ni las características de las interfases.

Características principales de SET: Las especificaciones de SET parten de una serie de criterios de diseño que permitan la mayor difusión y seguridad del protocolo. Estas características generales son:

- Estándar abierto
- Objetivo específico: Transferencia de números de tarjetas de créditos
- Utiliza codificación estándar (ASN.1 y DER)
- Independiente del medio de comunicación utilizado
- Utiliza estándares criptográficos ampliamente manejados (PKCS, X.509)
- Utiliza Criptografía de Clave Pública
- Autentificación basada en la certificación digital de todas las entidades participantes en la transferencia

4.1 Entorno: A diferencia de SSL, en SET se definen tres entidades independientes: Cliente (Cardholder), Vendedor (Merchant) y la Pasarela de Pago (Gateway Payment) que se interconectan directamente por Internet, haciendo el Vendedor de puente entre el Cliente y la Pasarela de Pago. Previamente a cualquier comunicación entre ellos, todas las entidades deben haber obtenido un certificado digital valido a través de la Autoridad de Certificación adecuada. La Pasarela de Pago permite la conexión desde Internet con las Redes Bancarias como VisaNet, dentro de estas Redes distinguimos otras dos entidades. El Issuer o entidad emisora de la tarjeta de crédito y el banco receptor de la transacción electrónica. SET se diseñó pensando en su utilización en Internet pero no de un modo exclusivo como SSL, sino que permite la conexión a través de cualquier tipo de red siempre que se definan los interfaces adecuados. Jerarquía de Certificación: SET es el primer proyecto de certificación a escala global que se va ha realizar en el mundo. Los certificados SET se estructuran siguiendo una jerarquía piramidal única que culmina en una Autoridad Certificadora Raíz (Root CA) que es la encargada de certificar a todas las demás autoridades certificadoras. Bajo la Root CA se encuentran las Brand CA o CA propiedad de las Entidades emisoras de Tarjetas de Crédito. Obviamente las primeras Brand CA's pertenecen a Visa Internacional y MasterCard Internacional. Las Brand CA's pueden a su vez certificar a otras CA's para que actúen en un ámbito político determinado, estas CA's reciben el nombre de Brand Geopolitical CA. En España, ACE (Agencia de Certificación Española) asumirá el rol de CA Brand Geopolitical para las tarjetas Visa y MasterCard así como CA emisora de certificados de Cardholder, Merchant y Gateway.

4.2 Autoridades de Registro: SET establece un protocolo para la obtención de certificados electrónicos. En la práctica la obtención de un certificado implica que la CA necesita estar segura de que el destinatario del certificado digital es realmente quien dice ser. Esta labor la llevaran a cabo las llamadas Autoridades de Registro, que actuarán de avaladores ante la CA de los usuarios y se encargarán de tramitar los certificados liberando al usuario final de gran parte de esta labor. Las Autoridades de Registro serán precisamente los bancos, esto permitirá que los certificados estén asociados a números de cuentas bancarias y no a personas físicas; permitiendo las compras anónimas, por lo menos desde el punto de vista del Vendedor.

4.3 Pago electrónico: El esquema de pago electrónico SET es muy similar al de CyberCash y, al igual que este, admite una gran variedad de opciones. En un pago normal SET, todo se inicia con una orden de pago

que el cliente envía al vendedor. Esta orden de pago esta dividida en dos: la descripción de la compra (OD) y los datos financieros del cliente (PIN). Estos datos se firman y se relacionan entre sí por medio de un algoritmo llamado Firma Dual. Los datos financieros van, a su vez, encriptados con la clave de la pasarela de pago por lo que no pueden ser consultados por el vendedor. El vendedor envía estos datos encriptados a la Pasarela de Pago que autoriza la transacción. Una vez autorizada, el Vendedor envía una respuesta al comprador firmado que sirve de comprobante de venta. Finalmente el vendedor realiza la captura del importe, es decir envía la orden al banco de que se efectúe la transacción.

4.4 Ventajas sobre SSL: SET ofrece una serie de mejoras sobre el sistema basado en SSL. Concretamente en lo referente a los servicios de seguridad podemos comentar lo siguiente:

- Confidencialidad: Al separar los datos financieros de la descripción de la compra aumentamos la confidencialidad ya que ni el vendedor ni el banco tienen acceso a datos que no le son imprescindibles
- Integridad: Todos los mensajes van firmados digitalmente de modo que se garantiza la integridad de todos los datos incluso tras finalizar la conexión.
- Autentificación: Todos los participantes están certificados por una Autoridad Certificadora única, lo que imposibilita cualquier tipo de usurpación de identidad así como la utilización de números de tarjeta de crédito robados
- No repudio: Los mensajes firmados pueden servir como Recibo de compra, sirviendo de prueba inalterable de que la transacción se produjo de un modo concreto.

Anexo 7

Redes

1 La necesidad de una red segura internet estas cambiando la manera como trabajamos, pero con la internet nos enfrentamos a riesgos nunca antes experimentados referentes a información de la institución, cada día se descubren nuevos tipos de ataques, los cuales cada vez son más prolíficos y más fáciles de implantar y fundamentalmente ocurren por varias razones entre las que podemos mencionar:

- La universalidad de Internet con millones de equipos y usuarios agregado al hecho de que se conforma una sociedad con todos los beneficios y problemas que un modelo social implica, medio en el cual por supuesto existen delincuentes y vándalos, que pueden compartir sus técnicas y conocimientos en un mundo sin frontera. Si simplemente en la Internet hacemos una búsqueda de los términos "hack", "crack" o "phreak", encontraremos cientos de sitios, muchos de los cuales códigos que nos indican como infiltrarnos o cometer diversos tipos de fechorías. A esto debemos agregar que los países no castigan de igual manera el delito electrónico y que la planificación del mismo no conlleva a ningún tipo de riesgo
- El segundo elemento a considerar viene dado por la gran facilidad de uso de los sistemas operativos y los ambientes de desarrollo, lo que hace que no se requieran de grandes estudios o conocimientos para llevar a cabo un ataque, todo ello hace que una persona puede desarrollar aplicaciones fáciles de usar y distribuirla a las masas de usuarios, lo que esta haciendo que para atacar una red tan sólo requerimos una dirección IP o el nombre de un host, y el clic de un ratón para iniciar un ataque en gran masa, ataque que cuando sea descubierto puede tener afectadas a miles de redes y cientos de miles de redes

2 ¿Qué es un "servidor Web seguro? En años recientes, la frase "servidor Web seguro" ha adquirido diferentes significados para distintas personas:

- ✓ Para los proveedores de software que los venden, un servidor Web seguro es un programa que instrumenta ciertos protocolos criptográficos, de forma que la información transferida entre el servidor y un navegador no pueda ser interceptada.
- ✓ Para los usuarios, un servidor Web seguro es el que resguarda toda la información personal que se reciba o recoja. Es un servidor que asegura su privacidad y no subvierte a su navegador para bajar virus a otros programas hostiles a su computadora.
- ✓ Para la compañía que lo administra, un servidor Web seguro es el que resiste determinados tipos de ataques, ya sean a través de Internet o de usuarios internos.
- ✓ Para nosotros, es la combinación de HW y SW que hacen a una máquina no vulnerable ante ataques de terceros, resguardando toda la información contenida en él. Un servidor Web se pude asegurar hasta el Firewall que evita intromisiones de personas dentro del servidor, porque del Firewall hacia la red, ya no queda de parte de parte de administrador del servidor ocuparse de esa seguridad.

Un servidor Web seguro es todo esto y más. Es un servidor confiable. Es un servidor que posee un espejo o que se respalda, de tal suerte que en caso de fallas de software o hardware puede restablecerse con rapidez. Es un servidor expandible, de forma que pueda dar buen servicio a grandes cantidades de tráfico.

Desafortunadamente, cuando los proveedores utilizan la frase "Servidor Web Seguro" por lo general se refieren a un servidor que instrumenta ciertos protocolos criptográficos, los cuales permiten a los navegadores y servidores Web intercambiar información sin riesgo de que la intercepten terceros que tengan acceso a los mensajes durante su recorrido. La encriptación hecha por tales protocolos es ampliamente reconocida como prerrequisito para el comercio en Internet.

Aunque los protocolos criptográficos son útiles para proteger información que viaja por Internet contra la intercepción, no son estrictamente necesarios para la seguridad en el Web, ni suficientes para garantizarla. Por ello, el término servidor Web con facilidades criptográficas es utilizado en vez de "servidor Web seguro" para denominar a un servidor Web que instrumenta protocolos criptográficos. A fin de comprender la distinción, se puede considerar la siguiente analogía, utilizada por Gene Spafford durante los últimos años:

Los servidores Web "seguros" son el equivalente de los carros blindados. El problema es que se utilizan para transferir tubos de monedas y cheques escritos con crayolas por gente sentada en bancas del parque a favor de comerciantes que hacen negocio sobre cajas de cartón debajo de los puentes de las autopistas. Además, los caminos tienen desviaciones aleatorias, cualquiera que tenga un desarmador puede controlar

los semáforos y no existe la policía. La seguridad en el Web requiere de mucho mas que la simple protección contra la intercepción.

3 El problema de la seguridad en el Web.- El problema de la seguridad en el Web consta de tres partes principales:

- Asegurar el servidor y los datos que contiene. Es necesario asegurarse de que el servidor pueda continuar operando, que la información que reside en el no sea modificada sin autorización y que sea distribuida sólo a quienes se desea distribuir.
- Asegurar la información que viaja entre el servidor Web y el usuario. Es deseable que la información que proporciona el usuario al servidor Web (nombre de usuario, claves de acceso, información financiera, etc) no pueda ser leída, modificada ni destruida por terceros. Muchas tecnologías de red son en particular susceptibles a la intercepción, ya que los datos se transmiten físicamente a todas las computadoras de la red de area local.
- Asegurar la computadora del usuario. Es necesario tener una forma de garantizar a los usuarios que la información, datos o programas descargados a sus sistemas no ocasionarán daños, de otro modo se mostraran reacios a utilizar el servicio. Además, es deseable tener una forma de asegurarse de que la información descargada sea controlada después, conforme el acuerdo de licencia de usuario y/o los derechos de autor.

Junto con todas estas consideraciones, pueden existir otros requisitos. Por ejemplo, en algunos casos existen los siguientes retos:

- ✓ Verificar la identidad.
- ✓ Asegurar que los mensajes sean enviados entre cliente y servidor en forma oportuna, confiable y sin repeticiones.
- ✓ Llevar bitácoras y auditar información sobre la transacción con propósitos de facturación, resolución de conflictos, no reclamo a investigación de uso incorrecto.
- ✓ Equilibrar la carga entre varios servidores.

Para responder de modo adecuado a tales preocupaciones es necesaria la interacción de varios de los componentes básicos, además de la red y sistema operativo subyacentes.

3 Taxonomía de un Ataque los ataques a las redes puede ser tan variada como los sistemas que tratan de penetrar, algunos son elaborados de una manera muy compleja, mientras que otros son llevados a cabo por un operador de manera no intencional o con desconocimiento de lo que esta haciendo. Es necesario entender algunas de las limitaciones inherentes a TCP/IP cuando evaluamos los diversos tipos de ataques. La Internet nace por la unión integral entre gobierno, entidades privadas y universidades, todos ellos con un objetivo en mente facilitar su conocimiento, uso e investigación. Los diseñadores nunca imaginaron la dispersión que Internet tendría, por esta razón en esa fase de desarrollo, la seguridad no tenía ninguna razón de ser es decir no fue considerada en su plan de desarrollo, mucho tiempo después de su implantación es cuando comienza a pensarse y a desarrollar medidas de seguridad, por esa razón de falla intrínseca de seguridad en su planificación es que se hace necesario la instauración de prácticas de seguridad en las redes, servicios y el análisis de productos que mitiguen los riesgos inherentes a IP, a continuación enumeramos los tipos de ataques que comúnmente ocurren en las redes y como estos ataques pueden ser mitigados.

3.1 Sniffers es un software de aplicación que utiliza una tarjeta de red en modo promiscuo para capturar todos los paquetes que son enviados a través de un dominio particular de colisión, son usados legítimamente en las redes para resolución de problemas y análisis de tráfico, debido a que en la actualidad muchas aplicaciones de redes reciben y envían datos en "Clear Text", un paquete de Sniffer puede capturar con suma facilidad información sensitiva además de palabras claves y nombres de usuarios, lo grave de esto es que gran cantidad de usuarios por razones prácticas utilizan una sola palabra para acceder a la red o la aplicación y un solo passwords. Debido a que los delincuentes de redes utilizan debilidades de la naturaleza humana para lograr a través de "Ingeniería Social" otro método de Sniffer que se torna sencillo para crear puertas de acceso desconocida por las personas encargadas de garantizar la seguridad de la red. Esta treta tiene varios esquemas que nos permiten protegernos contra su uso, entre ellas cabe mencionar:

- *Autenticación* les el primer nivel efectivo de defensa frente a un ataque de Sniffer, tal vez el mejor esquema de autenticación parte de la premisa de usar algo que me pertenece, que sólo yo conozco y que no puede ser duplicado

- *Switche de Infraestructura* esto hace que sólo pueda accederse a la información que fluye a través de un puerto específico al cual están conectados, si bien no elimina la treta reduce su efectividad
- *Herramientas anti-Sniffers* se basan en la detección de cambios en los tiempos de respuesta a fin de detectar si el host procesa más tráfico que el que normalmente maneja. AntiSniff[1] es una herramienta que hemos evaluado con excelentes resultados
- *Criptografía* es el método más efectivo ya que aunque no elimina la acción, hace inocuo el ataque

3.2 IP Spoofing es un ataque que ocurre cuando un atacante interno o externo pretende hacerse pasar por una dirección confiable, esto puede hacerse en una de las dos siguientes maneras, utiliza una dirección IP dentro del rango de direcciones confiables internas o externas de la empresa y con ello logra apoderarse de recursos específicos de una red. Normalmente este ataque tiene como objetivo el incluir data o comandos dentro de una cadena de información y por este método alcanzar un servidor o una conexión, logrado esto busca la obtención de comunicaciones bidireccionales para ello cambia las tablas de los Routers a fin de apuntar a la red a la que hace Spoofing. Otra metodología que se sigue para esta treta es simplemente recibir todos los mensajes que provienen de la dirección y posteriormente llevar a cabo la discriminación. Spoofing puede ser reducido pero no eliminado a través de las siguientes medidas.

- *Control de Acceso* mediante políticas que reduzcan la posibilidad de acceso desde una fuente externa usando como origen una fuente interna, pero si existen direcciones externas confiables este esquema no funcionará
- *Filtro RFC 2827* con ello negamos el acceso externo desde una dirección que no este dentro del rango de direcciones IP confiables, el ISP puede también implantar este tipo de filtro el cual es conocido como el Filtro RFC 2827. Este filtro niega el tráfico que no proviene de una fuente esperada para un Interface particular
- *Autenticación Adicional* tal como la especificamos anteriormente

3.3 Ataques de Negación de Servicio (DoS) ciertamente la más publicitada forma de ataque de DoS es la más difícil de ser eliminada, inclusive en el mundo Hacker esta treta es considerada como muy trivial por su fácil implantación y no requiere mayor esfuerzo, pero por estas mismas razones y por el amplio daño que ocasiona debe ser considerada de manera especial por los administradores de redes. DoS a diferencia de otros tipos de ataques no tiene como objetivo acceder y tomar posesión de la red, su objetivo es negar la disponibilidad o retardar el acceso de la información al atacar recursos limitados de la red tales como el ancho de banda. Muchos de los ataques de Dos se aprovechan de las vulnerabilidades de la arquitectura de redes. Este tipo de ataque es el más difícil de contrarrestar, se detecta por un incremento inusitado del ancho de banda y en muchos casos proviene de varias fuentes dicho ataque con el fin de sacarlo de servicio por un amplio espacio de tiempo. Pude ser mitigado utilizando las siguientes técnicas

- *Herramientas Anti Spoofing* tal como lo analizamos en el punto anterior
- *Herramientas Anti Dos* esto se hace al nivel de firewalls o Routers a fin de disminuir la efectividad de estos ataques, en muchos casos trabaja sobre un esquema de Periodo de Vida Media, con alarmas de consumición de ancho de banda
- *Limitación Tráfico* se puede limitar el tráfico al nivel de ISP, podemos limitar por ejemplo en un momento dado el tráfico de ICMP que se utiliza sólo para razones de diagnóstico

3.4 Ataques de Password es otro de los ataques preferidos, para ello se utilizan diversos métodos, desde los ataques de fuerza bruta, Troyanos, Spoofing, Sniffers. Usualmente su característica viene dada por múltiples ataques que son repetidos en muchos casos de manera automática con el objetivo de descubrir la cuenta del usuario y el passwords. Los ataques de Fuerza Bruta es llevado a cabo usando un programa que corre en la red y que intenta hacer login en algunos de los recursos de la red, especialmente estaciones de trabajo y servidores, cuando se logra acceder la red, se tienen los mismos derechos que el usuario al que se suplanta. Nuevamente en este punto debemos tocar un hecho que ya se ha hecho costumbre y es que normalmente el usuario tiene asociadas todas las aplicaciones a un login y un password, por lo tanto si logra el acceso a un recurso con el puede ir adquiriendo recursos adicionales.

El Ataque de Password puede ser eliminado fácilmente, reemplazando la facilidad de un password establecido en Clear Text, por uno de los que utilizan tecnología de Token, o la tecnología de autenticación que ya hablamos al momento de prevenir los ataques por Sniffers, pero desafortunadamente muy pocas instituciones pueden hacerlo, aunque la que en este instante estudiamos al aprobar la tarjeta inteligente como forma de autenticación ante la institución se hace fácil llevar a cabo el proceso al nivel de integrarlo

[1] www.10pht.com/antisniff//

usando lectoras y a un costo relativamente bajo al área de prevención y control de acceso. Pero mientras esto se logra es necesario imponer una política de password que incluya letras en mayúscula y minúscula, números y caracteres especiales, además de esto debemos agregar que tras un número de intentos, pase un largo tiempo antes de que la persona que trate de acceder pueda hacerlo nuevamente. Utilizando la herramienta L0phtCrack, pudimos acceder a 85 de 100 máquinas en la institución a las cuales atacamos a fin de determinar la fortaleza de la política de password que actualmente se viene utilizando.

3.5 Ataque de "Man-in.the-middle" supone que el intruso tenga acceso a los paquetes de la red y a través de ellos pueda entrar a nuestros recursos, estos ataques son llevados a cabo generalmente usando Sniffers conjuntamente con transporte de protocolos y Routers, se utiliza este ataque principalmente para robar información o ganar acceso a recursos privados, su mitigación sólo es posible por el uso de alguna técnica de criptografía

3.6 Ataque a niveles de aplicación puede implantarse utilizando diversos medios, uno de los más comunes es explotando las bien conocidas debilidades del software instalados en los servidores tales como "http" y "FTP", al explotar estas debilidades se puede ganar acceso con todos los permisos de la persona que viene corriendo la cuenta y así utilizar los privilegios que posee, normalmente el atacante utiliza puertos permisados por el Firewall come el puerto 80, estos tipos de ataques no pueden ser eliminados ya que nuevas formas de ataques constantemente van apareciendo, pero si tenemos buenas maneras de administración podemos evidentemente disminuir los riesgos, a continuación pasamos algunas medidas que pueden ser tomadas:

- Revisar los logs utilizando para ello herramientas automáticas que fácilmente nos permitan detectar desviaciones, en este instante estamos evaluando la herramienta PERL que está ubicada en www.activestate.com
- Suscribirse a paginas que publica vulnerabilidades y contramedidas tales como Bugtraq en www.secutityfocus.com o CERT en www.cert.org
- Mantener el sistema operativo y las aplicaciones con los últimos patches
- Utilizar herramientas de IDS(Intrusión Detection System) presentan una nueva tecnología aparecida aproximadamente hace tres o cuatro años, y esta prometiendo revolucionar el mercado de acuerdo con la visión de algunos vendedores, de hecho una empresa se ha atrevido a pronosticar que IDS a corto plazo reemplazará los Firewalls, pero desde nuestro punto de vista esto no se cumplirá ya que IDS es una vía para incrementar la seguridad de la red, no para reemplazar ninguno de los mecanismos existentes.

Preguntas frecuentes acerca de IDS para entender IDS, debemos imaginar un sistema compuesto con un Data Analizer y un observador que vigila la información que pasa a través de él, este observador conoce acerca de los últimos tipos de ataques existentes y cual es su comportamiento, con esto en mente revisa de manera diligente todo la información que pasa por la red, si encuentra o determina algo sospechoso, automáticamente contacta al administrador de la red y le informa acerca de lo que ha encontrado. Por ejemplo si un sistema IDS detecta que un host de una manera repetida esta enviando paquetes SYN a otro host, sin tratar de completar la conexión, el IDS detecta que se esta llevando a cabo un ataque y toma las acciones apropiadas. Un buen IDS, tiene grabados en su base de datos más de 100 patrones de ataques, y las acciones que toma, dependen de el sistema que se estén utilizando y de su configuración. Todos los sistemas de IDS pueden mantener un Log, de los eventos sospechosos, algunos además tienen un paquete que captura la información para que posteriormente pueda ser analizado por el administrador de la red, otros pueden ser configurados de manera que puedan enviar un mensaje al detectar algún tipo de ataque, otros al detectar el ataque cortan la comunicación que se ha establecido y finalmente existen otros capaces de interactuar con el Firewall a fin de modificar las reglas de acceso y bloquear el ataque del cual esta siendo objeto.

Un IDS esta conformado por dos subsistemas.

La máquina, que es responsable de capturar y analizar el tráfico

La consola, desde la que podemos operara la máquina y pueden obtenerse los reportes deseados.

Una cosa debe tomar en cuenta con estos equipos y es que consumen gran cantidad de recursos. Típicamente estos equipos corren en máquinas dedicadas con un mínimo de 128 MB de RAM y un procesador Intel de 300MHZ, en caso de un equipo corriendo en UNIX, se requiere una máquina RISC, si se hace un Log de todo el tráfico que pase, se requiere una alta capacidad de disco para grabar los mensajes.

Limitaciones de los IDS a pesar de que podemos verlos como equipos de gran potencia y que se puede creer vienen a solucionar gran parte de los problemas de seguridad, pero en realidad presentan uno que es difícil de solucionar y viene dado en que las decisiones son tomadas en tiempo real, lo que hace que algunas medidas que se tomen sean muy tarde.
Entre las variedades de IDS podemos encontrar:

- NIDS que hace seguimiento a paquetes sospechosos y ante ciertos eventos lanza una alarma, snort es un programa que he evaluado que permite detección de intruso, es gratuito y puede obtenerse en www.snort.org
- HIDS nos permite pasar a la ofensiva cuando se intente rastrear la red y permite registrar solicitudes, y generar respuestas falsa

4 Reconocimiento de Redes se refiere a la obtención de información de una red, utilizando información disponible y aplicaciones. Cuando se desea penetrar una red se busca conocer lo máximo posible de la misma antes de lanzar un ataque, para ello utilizan DNS, que es uno de los servicios que casi siempre es necesario y que se ejecuta en cualquier red perimetral de internet, un alto porcentaje de los servidores DNS conectados a Internet presentan alta vulnerabilidad, la información suministrada por DNS nos revela la vida del dominio, si a esto agregamos un escaneo de puertos, obtendremos los servicios disponibles. Utilizando herramientas de IDS, nos es posible detectar este tipo de ataques, otra manera es negando información utilizando comandos de ICMP tales como apagar las funciones de echo y echo reply
4.1 Explotando la Confianza aunque no es un ataque directo estamos hablando de una ataque que realiza un individuo aprovechándose de la confianza y buena fe, un clásico ejemplo es un ataque perimetral que aprovechándose del hecho de estar en el mismo segmento de red y teniendo frecuentemente acceso a servidores de DNS, http, SMTP, introduciéndose en uno de estos sistemas y valiéndose de la relación de confianza puede acceder a otros que no le están permitidos, utilizando firewalls entre estos dominios disminuimos la incidencia de estos ataques, aplicando la medida que no debemos confiar de la persona que se encuentra fuera del Firewall, a esto debemos agregar las políticas de control de acceso ya mencionadas con anterioridad.
4.2 Redireccionamiento de Puertos La seguridad estándar que recomendamos para los Routers de la institución comprende los siguientes aspectos:

- **Negar rutas RFC 1918** define los rangos de direcciones IP disponibles para ser usadas en Internet así como las que se consideran privadas, es decir aquellas no usadas por Internet, muchos de los ataques utilizan estas direcciones privadas
- **Servidores UDP y TCP** son generalmente servidores con número de puertos por debajo de 10 que incluyen puertos de "ECHO" que es usados para ataques de negación de servicio, para ello simplemente podemos desactivarlo con los comandos de "no-service-udp-small-server" y el mismo comando reemplazando udp por tcp.
- **Finger Service** se utiliza para resolver usernames o remote systems, Finger muestra los usuarios activos de un sistema, para su restricción el comando que debe usarse es "no service finger"
- **IP Unreachables** por defecto cuando un router recibe un mensaje que no puede ser manejado o es un mensaje no reconocido se envía un mensaje de ICMP a la fuente que originó el mensaje, si bien este comportamiento es razonable, puede que el router empiece a desperdiciar recursos contestando mensajes lo que podría ocasionar un ataque por negación de servicio, debe utilizarse el comando "no IP unreachable", para evitar este ataque.
- **ICMP Redirect Messages** bajo ciertas circunstancias los Routers no tienen un comportamiento optimo, aunque podemos mejorar esta falla con una configuración conveniente, es muy conveniente que un mensaje no se envíe fuera de los limites de donde fue enviado. A través de ICMP el que envía el paquete original que elimine la ruta definida por otra que supuestamente es más conveniente, la negación de esto se puede hacer por el mensaje "no ip redirects"
- **Directed Broadcast** es posible enviar un mensaje que empacado permite reenviar a otro Interface, esto se evita mediante el comando "no ip Directed-Broadcast"

5 El Programa de Auditoria dado que en anexos anteriores nos concentramos en aspectos de comunicación, en este anexo nos referiremos específicamente a la auditoria de los equipos que conforman la red a nivel de capas 2 y 3, el programa de auditoria se avocara a los siguientes objetivos:

- Identificación de todos los Bridges, Gateways, Routers y Hubs en la red

- Identificar todas las direcciones aprobadas de IP
- Revisar el output de las direcciones de output de los Routers, Firewalls o Hubs a fin de determinar si existen salidas no usuales
- Revisar y comprobar la efectividad de los filtros que estamos utilizando
- Identificar cualquier técnica que pueda ser utilizada para evitar la acción de los firewalls o Routers
- Identificar conexiones de servicios externos no protegidas
- Identificar todas las transacciones que se realizan a través de la red y asegurar que cumplen con el grado de control exigido por el usuario
- Preparar tretas que puedan evitar la protección de los equipos, asegurar que las mismas son detectadas

6 Control de Riesgos para Bridges, Router y Firewalls

Riesgo	Control
Los equipos Switch no están propiamente asegurados. En las revisiones rutinarias de seguridad estos equipos no son cubiertos, por tanto los riesgos que de ello se derivan no han sido comprobados	Los Switches de la red deben ser seguros. Al menos una vez al año debe ejecutarse una rutina de control a fin de asegurar que los controles están instalados y que continúan teniendo vigencia
Algunos equipos de Switch, frecuentemente no están protegidos por password o tienen el password que por defecto proporciona el usuario. Adicionalmente algunos Switches están conectados a módems de Dial-up, para permitir el acceso remoto a cierto personal. Cuando combinamos estos aspectos estamos posibilitando a que un externo tome control de la Instalación	Todos los equipos deben estar protegidos por passwords, que eviten cambios en la configuración definida, adicionalmente los accesos a través de módems deben estar plenamente justificados y su acceso debe hacerse por passwords Tokens
Los Bridges unen redes y permiten el flujo de la información entre ellos, sin ningún tipo de filtrado	Sólo redes pequeñas deben estar conectadas por medio de bridges y los mismos deben permanecer tan aislados como sea posible
Los Bridges dejan pasar todos los mensajes y podrían degradar el tiempo de respuesta de la red. Los bridges están muy expuestos a los ataques por negación de servicio por mensajes de Broadcast, además ellos son los equipos que operan a menor velocidad en la red	Reemplace cuando sea posible los Switches por Routers en la medida en que se incrementan los servidores, o si la red no esta aislada
Los suplidores y sus técnicos frecuentemente requieren de accesos remotos a través de router, ellos pueden reprogramarlos y hacer upgrades de software, el resultado de ello podría ser cambios sin consulta o penetración a la red de la institución	Desconecte la capacidad de acceso de este personal, y cuando requieran conectarse, supervíselo a través de procedimientos manuales. Instale procedimientos de autenticación en donde exista la posibilidad de acceso remoto, revise las tablas a fin de determinar todas las direcciones que pueden accederlo, investigue las direcciones desconocidas o poco usuales
Los Routers comparte su información para hacer más eficiente la transferencia de información	Asegurese que todos los Routers y que cumplen con los convenios de seguridad establecidos, compruebe esto antes de llevar a cabo la conexión
Las tablas de Routers tienen direcciones no autorizadas	Baje las tablas a un archivo plano, verifique todas las direcciones, siga esta rutina con frecuencia y compare la información almacenada en los archivos, identifique las diferencias encontradas y busque la explicación del motivo de estas diferencias
Personas no autorizadas podrían estar navegando en nuestra red, ocasionando graves problemas en	Instale verificadores de cuentas en los Routers, baje la información referente a cuentas a un archivo

nuestros archivos, además pudieran insertar programas o virus	plano, identifique cualquier cuenta que tenga un uso poco común Algunos Routers no tienen esta capacidad, cuando requiera equipo nuevo o haga un upgrade solicitela
Los router dinámicos intercambian su información, esto puede traer como consecuencia que información no autorizada sea enrutada a través de la red	Monitoree las direcciones de las tablas de los Routers y use la cuenta para identificar actividad inusual. Además los Routers dinámicos pueden programarse para que no permitan que direcciones no autorizadas sean intercambiadas, cuando este sucede debe enviarse un mensaje de Broadcast a los administradores de la red
Los password por defecto de los Routers son conocidos, están disponibles tanto en manuales como en la Internet, además en muchos casos esta actividad no esta encendida	Siempre que se instale un router cambie el password que trae por defecto, active la actividad de password, al menos cada seis meses cambie los password de la red, hágalo también después de que se haga un cambio mayor en la misma
La configuración de los Routers es almacenada con frecuencia en servidores o en estaciones, un externo que penetre la red puede obtener estos archivos y con ellos adueñarse de la red.	No suministre nombres obvios a estor archivos, no use la marca de referencia como parte del archivo, Encripte la información que tiene almacenada
Es frecuente que cuando alguien penetra la red, los administradores de la red le cierran el punto de acceso pero no reportan el incidente, puede ser que el infractor creara back doors y que al cabo de algún tiempo volvieran a penetrar la red	Cuando alguien penetra la red debe reportarse, hacerse una exhaustiva auditoria para identificar como entraron, que actividad realizaron y si dejaron pistas para entrar nuevamente
Una red interna ha sido penetrada, esta poniendo en peligro toda la red	Toda la información crítica debe estar encriptada Instale Firewalls entre las redes si una de ellas no es confiable, además si es posible instale firewalls entre la red y los servidores que tienen información sensitiva
En algunos casos los filtros que utilizamos no actúan como lo esperamos, motivado a que no esta propiamente codificado	Realice frecuentes tormentas de ideas a fin de determinar como un filtro pudiera ser evitado, y si detecta debilidades revise la programación y cámbiela por una que sea más efectiva.
Algunas conexiones externas no están provistas de Firewall o Proxy, como consecuencia de ello están en alto riesgo	Todas las conexiones externas deben estar provistas de un Firewall o Proxy que las proteja, adicionalmente debe tratar de penetrarla con cierta frecuencia a fin de comprobar su efectividad
Mucha gente piensa que los firewalls lo protegen contra los ataques de externos, esto agrega un peligro ya que supone que se tiene seguridad pero la misma no esta fundamentada, el exceso de confianza es peligroso cuando hablamos de seguridad	Es necesario educar a los usuarios e indicarles los riesgos a los que esta expuesta la información
Los Firewalls pueden ser evitados por medio de conexiones no autorizadas a través de estaciones de trabaja o redes LAN, también puede estar comprometida por router o servidores débilmente configurados	Realice un inventario de las PC´s y el software/hardware que tiene instalado, proteja los equipos contra instalaciones, trate de identificar software tales como GOPHER, MOSAIC, CIM. Utilice la capacidad de detección de cuentas de los firewalls para detectar volúmenes información no usual o direcciones desconocidas Use un programa de Demon para identificar módems no autorizados, verifique estos aspectos con cierta regularidad

Puede ser que el Firewall evite una penetración, pero usando Ping pude hacer un mapa de su red interna, pueden obtener otra información adicional usando finder y tftp, en caso de negación de servicio pueden usar echo o chargen	Ping, tftp y Zinder, echo y chargen deben ser deshabilitados
La red puede ser penetrada y usada para almacenar información no deseada, muchos administradores no investigan este modo de penetración	Diariamente debe monitorearse la información contenida en los servidores, buscar por archivos escondidos, por archivos nuevos con mucha actividad, debe proveerse una nomenclatura de archivos que permita identificar quien lo creo, los archivos temporales, deben ser borrados al cumplir con su periodo, debe hacerse seguimiento a los archivos avi, bmp, jpeg
La data critica almacenada en servidores de ftp, no esta protegida de manera apropiada	Corra un programa en el servidor de ftp varias veces al día para identificar archivos que no están protegidos contra lectura o escritura
Las transacciones críticas tales como pagos, matriculas y otras sensitivas, puede que no estén bien protegidas, mientras viajan a través de la red	Las transacciones sensitivas deben ser encriptadas, mientras están en transito
Los passwords de los clusters de Internet no son suficientemente fuertes para prevenir un ataque	Correr programas que actúen como ataques de fuerza bruta para detectar estas debilidades, todo password descubierto debe ser reemplazado
Los usuarios internos atentan burlar el Firewall llamando al ISP local	Monitoree llamadas locales a fin de identificar números de ISP, identifique de donde provienen los números y actué sobre los infractores
Algunos usuarios abusan de los privilegios de Internet	Revise diariamente los logs del Firewall, a fin de determinar que sites visitan y el tiempo que permanecen conectados a los mismos, esto puede efectuarse de manera automática ya que algunos firewalls ofrecen este tipo de servicio, en caso de que esto no sea así un simple programa manejando archivos planos nos permite obtener esta información
El administrador no esta al tanto de que esta siendo atacado y por tanto no toma acciones correctivas a tiempo	Instale paquetes como RealSecure, Intruder Alert, Web Stalker, para determinar intentos de penetración por internet
Monitores no autorizados mapean la red, como no dan ningún mensaje el administrador no los detecta	Use un monitor de red, que identifique direcciones poco usuales, o un significativo volumen de mensajes supervisorios a direcciones específicas

7 Políticas de Acceso Remoto Acceso remoto significa que nuestras redes comienzan a ser más abiertas, estamos en algunos casos incrementando el número de usuarios que trabajan desde puntos externos. Cuando tenemos acceso remoto no estamos bajo el fácil control administrativo de una LAN, el equipo esta ubicado en puntos fuera de las oficinas de la institución, además pasamos por enlaces públicos que a su vez son vulnerables en exceso. La seguridad por tanto debe comenzar por la propia red antes de dar acceso a la información propiamente dicha. *Cuando los equipos y conexiones de acceso remoto, representan un sólida línea de defensa, un potencial sabotaje no tendrá mucha oportunidad de ser llevado a cabo.*

Las Políticas de Seguridad de una conexión vía acceso remoto deberá cumplir con los siguientes objetivos:

- Proveer una adecuada Seguridad
- Proveer una fácil administración
- Ser transparente para los usuarios

En base a ello establecemos la siguiente política:

1. Acceso Remoto es una facilidad que se ha introducido para permitir a *cierto* personal autorizado, administrar y dar soporte a las funciones y procesos que se encuentran bajo su control y enmarcadas estrictamente en funciones de la institución
2. Las Políticas de Acceso Remoto deberán ser revisadas y actualizadas por lo menos una vez al año, de forma tal que puedan reflejar los cambios tecnológicos, de esta manera aseguramos que la inclusión de nuevos productos no afectaran a la institución por la obsolescencia de estas políticas. La organización de INFOSEG, será la encargada de su actualización
3. Toda conexión de acceso remoto, debe cumplir con las políticas de seguridad vigentes(Anexo 2)
4. Todo usuario de acceso remoto, debe firmar un documento de uso y conexión, en donde especifica que conoce y entiende las políticas establecidas. El Administrador Descentralizado, será el encargado de tramitar el documento que deberá ser aprobado por la máxima autoridad de la organización
5. Todo usuario de acceso remoto deberá estar entrenado en aspectos de seguridad de información, será responsabilidad de INFOSEG proveer periódicamente este entrenamientoLa conexión remota debe ser realizada con fines que exclusivamente representen a la organización, otro tipo de actividad esta explícitamente prohibida.
6. Es responsabilidad del usuario la protección de la información y divulgación de la misma, que pudiere ser obtenida por medio de un acceso remoto
7. Los usuarios a conexión remota, deberán cumplir con las políticas en cuanto a password, control de acceso, auditoria, integridad y transferencia de información
8. El usuario al conectarse recibirá información acerca de la fecha y hora de su ultima conexión, de existir alguna discrepancia deberá informar de la manera más expedita posible a su Administrador Descentralizado.
9. Para efectos de seguridad se debe identificar cada uno de los usuarios de acceso remoto así como el puerto por donde efectuó la conexión
10. Esta prohibida todas conexión "Dial out", desde las redes internas de la institución
11. Las facilidades de Virus Scanning deben estar instaladas en la estación del cliente, estas deben ser actualizadas cada 15 días, todo ello acorde con las políticas antivirus establecidas(anexo 8)
12. Los usuarios de acceso remoto están de acuerdo con que la institución instale en sus equipos mecanismos de seguridad, con propósitos de autenticación y seguimiento
13. Las siguientes acciones están expresamente prohibidas al realizar una sesión de acceso remoto
    a. Evadir la autenticación
    b. Automatizar la sesión de Dial In
    c. Instalar y copiar software de aplicación, o de la institución sin consentimiento
    d. Desmantelar o acceder a el hardware de seguridad que pudiera instalarse en su equipo
    e. Permitir el acceso o revisión de la información por personal no autorizado
14. La facilidad de correo electrónico es para uso exclusivo para asuntos relacionados con la institución
15. Los sistemas que manejan información clasificada como confidencial no podrán ser accedidos por vía de acceso remoto. De requerirse su utilización la información deberá ser encriptada y accedido vía firma electrónica
16. Los usuarios de este servicio sólo podrán acceder a la información que explícitamente se le permita
17. Se utilizaran los siguientes métodos de autenticación:
    a. Identificación única por usuario
    b. El usuario tiene restricciones para acceder la información
    c. Debe cumplir con las políticas y normas establecidas
    d. Si el número de intentos no exitosos excede de tres se suspende el acceso, sólo el administrador descentralizado de la organización podrá reactivarlo
    e. Se pondrá en uso uno de los siguientes esquemas de autenticación
        i. Password dinámico
        ii. Callback
        iii. Protocolos de acceso específico
        iv. Reconocimiento de voz
        v. Identificación del número telefónico entrante

Matriz de Evaluación Tecnológica
Productos Antivirus

	Porcentaje Máximos	Mc Afee	Pc Clin	Dr Solomon	Norton
Degradación	13	12.5	10.0	13.0	12.0
Evaluación Tecnológica	13	12.7	11.0	12.0	13.0
Ofrece Scan de Memoria	4	3.0	2.0	3.5	4.0
Ofrece Scan de Archivos entrantes	5	5.0	5.0	5.0	5.0
Ofrece Scan en sectores de Boot	5	5.0	5.0	5.0	5.0
Ofrece adiestramiento	5	5.0	5.0	5.0	5.0
Ofrece apoyo en instalación	4	4.0	3.0	3.5	4.0
Actualización automática en Estación de Trabajo	4	3.0	2.5	2.5	3.0
Aviso de error	5	5.0	5.0	4.5	5.0
Ofrece upgrade sin costo	4	4.0	3.0	3.0	4.0
Trabaja en todas las plataformas(NT, Windowsxx, Linux)	5	5.0	5.0	5.0	5.0
Detecta virus encriptados	3	3.0	2.0	3.0	3.0
Ofrece actualizaciones adicionales	5	5.0	5.0	0.0	5.0
Detecta viruis en ZIP	4	3.5	2.0	3.0	4.0
Permite auditar estaciones	4	4.0	4.0	4.0	4.0
Incluye herramientas de desinstalación	2	2.0	2.0	2.0	2.0
Produce reportes de Scan	2	2.0	2.0	2.0	2.0
Porcentaje de reparación en archivos dañados	2	2.0	2.0	2.0	2.0
Help desk 24x7x365	4	3.8	3.9	3.8	3.8
Actualización por red	2	2.0	2.0	2.0	2.0
Detección y repación inclusive macrovirus	5	4.6	4.5	4.6	5.0
Totales		96.1	94.9	88.4	97.8

- Symantec Corp.
- Thunder Byte

Anexo 8

Virus

8.1 Historia de los Virus. Hacia finales de los años 60, Douglas McIlory, Victor Vysottsky y Robert Morris idearon un juego al que llamaron *Core War*, que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios Bell de AT&T. El juego consistía en que dos jugadores escribieran cada uno un programa llamado *organismo*, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera. Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un *organismo* suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas destinados a dañar en la escena de la computación. Desde esa época se mantuvo el conocimiento de los programas virales en un estado latente y aunque existían en su concepción muy poco se propago, en 1982, un hijo de Morris, pública en un periódico underground en Los Angeles, el trabajo que realizo su padre y el potencial que el mismo podría tener para atacar a los mini computadores que para esa fecha estaban saliendo al Mercado.

"El primer caso público de amplio espectro, se dio a conocer en Alemania, en 1987. Varios estudiantes de la Universidad de Clausthal-Zellerfeld se encontraron en su correo electrónico una carta llamada "Christmas", junto a un archivo ejecutable. En la carta se auguraba una sorpresa navideña para quien pusiera en marcha el programa. Los alumnos lo hicieron y les apareció el dibujo de un árbol de navidad adornado. Pero no sabían que, además del dibujo, accionaron el programa para que leyera sus agendas electrónicas y se enviara a sí mismo a todos los amigos de los estudiantes. El virus se llamó "IBM Christmas Tree", porque corrió devastador por las oficinas de IBM y, en poco tiempo, llegó al Japón." Un registro adicional que se tienen de una infección data del año 1987, cuando en la Universidad estadounidense de Delaware notaron que tenían un virus porque comenzaron a ver "© Brain" como etiqueta de los disquetes. La causa de ello era Brain Computer Services, una casa de computación paquistaní que, desde 1986, vendía copias ilegales de software comercial infectadas para, según los responsables de la firma, dar una lección a los piratas. Ellos habían notado que el sector de booteo de un disquete contenía código ejecutable, y que dicho código se ejecutaba cada vez que la máquina se inicializaba desde un disquete. Lograron reemplazar ese código por su propio programa, residente, y que este instalara una réplica de sí mismo en cada disquete que fuera utilizado de ahí en adelante.

Para la misma fecha, un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. Escribió una demostración de este efecto a la que llamó VIRDEM, que podía infectar cualquier archivo con extensión **.COM**. Esto atrajo tanto interés que se le pidió que escribiera un libro, pero, puesto que él desconocía lo que estaba ocurriendo en Pakistán, no mencionó a los virus de sector de arranque (boot sector). Para ese entonces, ya se había empezado a diseminar el virus Viena.

Actualmente, los virus son producidos en cantidades extraordinarias por muchisima gente alrededor del planeta. Algunos de ellos dicen hacerlo por divertimento, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

con relación a la motivación de los autores de virus para llevar a cabo su obra, supongo que cae dentro de alguno de los siguientes concepto.

- Algunos de los programadores de virus, especialmente los mejores, sostienen que su interés por el tema es puramente científico, que desean averiguar todo lo que se pueda sobre virus y sus usos.
- A diferencia de las compañías de software, que son organizaciones relativamente aisladas unas de otras (todas tienen secretos que no querrían que sus competidores averiguaran) y cuentan entre sus filas con mayoría de estudiantes graduados, las agrupaciones de programadores de virus están abiertas a cualquiera que se interese en ellas, ofrecen consejos, camaradería y pocas limitaciones. Además, son libres de seguir cualquier objetivo que les parezca, sin temer por la pérdida de respaldo económico.
- El hecho de escribir programas vírales da al programador cierta fuerza coercitiva, lo pone fuera de las reglas convencionales de comportamiento. Este factor es uno de los más importantes, pues el

sentimiento de pertenencia es algo necesario para todo ser humano, y es probado que dicho sentimiento pareciera verse reforzado en situaciones marginales.

- Por otro lado, ciertos programadores parecen intentar legalizar sus actos poniendo sus creaciones al alcance de mucha gente, (vía Internet, BBS especializadas, etc.) haciendo la salvedad de que el material es peligroso, por lo cual el usuario debería tomar las precauciones del caso.
- Existen programadores, de los cuales, generalmente, provienen los virus más destructivos, que alegan que sus programas son creados para hacer notoria la falta de protección de que sufren la mayoría de los usuarios de computadoras.
- La gran mayoría de estos individuos son del mismo tipo de gente que es reclutada por los grupos terroristas: hombres, adolescentes, inteligentes.

En definitiva, sea cual fuere el motivo por el cual se siguen produciendo virus, se debe destacar que su existencia no ha sido sólo perjuicios: gracias a ellos, mucha gente a tomado conciencia de qué es lo que tiene y cómo protegerlo.

8.2 ¿QUÉ ES UN VIRUS? Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o sector de "booteo" y se replica a sí mismo para continuar su esparcimiento. Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Se ha llegado a un punto tal, que un nuevo virus llamado W95/CIH10xx, también conocido CIH.Spacefiller (puede aparecer el 26 de cada mes, especialmente 26 de Junio y 26 de Abril) ataca al BIOS de la PC huésped y cambiar su configuración de tal forma que se requiere cambiarlo. Nunca se puede asumir que un virus es inofensivo y dejarlo "flotando" en el sistema.
Existen ciertas analogías entre los virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas-rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras, reproduciéndose una y otra vez cuando se accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento del ordenador.
Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: ***PROPAGARSE***. Es importante destacar que *el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.*
La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

- **D**añino
- **A**uto reproductor
- **S**ubrepticio

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas. Asimismo, se pueden distinguir tres módulos principales de un virus informático:

- Módulo de Reproducción
- Módulo de Ataque
- Módulo de Defensa

El **módulo de reproducción** se encarga de manejar las rutinas de "inoculación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.
El **módulo de ataque** es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus **Michelangelo**, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco duro volviéndola inutilizable.

El **módulo de defensa** tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

8.3 Ciclo de vida de un Virus. Los virus de computadoras así como los biológicos, poseen ciclos de vida que aquí describimos:

- **Creación:** Esta se produce cuando una persona con conocimiento de assembler trabaja en su gestación por varias semanas y termina creando un nuevo virus que se encuentra programado para reproducirse rápidamente y hacer daño en algún momento determinado especificado por el programador.
- **Gestación:** Describe el proceso por el cual el virus se aloja en un sector determinado con el propósito de futuras reproducciones. Usualmente esto es hecho en un programa muy usado ubicándolo luego en una BBS o distribuyendo copias a través de la oficina, escuela, etc.
- **Reproducción:** Los virus, por su propia naturaleza, se replican. Un virus con un buen diseño se replicará por un largo tiempo antes de que sea activado.
- **Activación:** Los virus que poseen rutinas de destrucción de datos se activarán cuando ciertas condiciones sean dadas. Algunos virus se activan en una fecha determinada mientras que otros poseen una especie de conteo regresivo interno de tiempo. Pero, aunque ciertos virus no tengan rutinas de daño (con lo cual sólo se reproducen), deben considerarse igualmente destructivos, ya que toman recursos del sistema.
- Descubrimiento: Esta fase del ciclo de vida del virus, no necesariamente tiene porque producirse luego de la activación, pero usualmente sucede de esta manera. Esto se produce cuando alguien da la noticia de un nuevo virus. Usualmente, pasa a manos de la NCSA (National Computer Security Association) en Washington DC y es documentado y distribuido a diseñadores de antivirus.
- **Asimilación:** Luego del descubrimiento, los diseñadores de software modifican sus productos para incluir la detección del nuevo virus.
- **Erradicación:** Si los suficientes diseñadores de antivirus son capaces de detectarlo y limpiarlo así como los suficientes usuarios adquieren el antivirus apropiado para combatirlo el virus puede estar cerca extinguirse. A pesar de que, ningún virus ha desaparecido por completo, algunos han cesado por largo tiempo de aparecer en la comunidad informática

8.4 Tipo de Virus: si bien esto puede cambiar de acuerdo a la propia evolución que presentan los virus, al momento podríamos hablar de los siguientes tipos de virus

- ✓ VIRUS DE AYUDA: Se esconden en los ficheros con formato HLP (formato de ayuda utilizado en programas bajo Windows)
- ✓ VIRUS DE BOOT, SECTOR DE INICIO, BSV ó MBR: Antiguamente el mas extendido, afectan a disquetes y discos duros, infectando el sector de inicio. Ejemplo VIRUS BARROTES, BRAIN. VIRUS DOS: Infectan los archivos BAT, EXE, COM del sistema operativo MSDOS, al ejecutarse, contagian a los demás ficheros.
- ✓ VIRUS WINDOWS: Como los VIRUS DOS, pero en este caso, los archivos ejecutables WIN32.
- ✓ VIRUS MULTIPLATAFORMA: Con diversos métodos como macros o infección archivos ejecutables, son capaces de infectar ordenadores con distintos sistemas operativos.
- ✓ VIRUS MULTIPARTITE: Infectan sectores de arranque pero además ficheros ejecutables.
- ✓ VIRUS DE SCRIPT: Escritos en lenguaje de Script como Visual Basic y se transmiten por correo electrónico o chat, aprovechando que hay programas que ejecutan estos script. Como ya se ha dicho anteriormente, estos son en la actualidad los más peligrosos. Ejemplo Virus Love Letter
- ✓ VIRUS DE MACRO: Son los que se ocultan en las macros. Las macros son "mecanizaciones" aplicadas a ficheros de texto. Así, existen macros en los procesadores de texto, hoja de cálculo y bases de datos. Ejemplo Virus Melissa.
- ✓ VIRUS CONSTRUCTORES: Es el que en su código contiene instrucciones para crear otros virus más pequeños, que van infectando los archivos.
- ✓ VIRUS POLIMORFICOS: Son quizás los más difíciles de detectar y en consecuencia de eliminar. Sus valores en la programación van cambiando secuencialmente cada vez que sé auto encriptan, de tal forma que sus cadenas no son las mismas. El virus polimórfico produce varias, pero diferentes copias de sí mismo, manteniendo operativo su micro código viral. Un fácil método de evadir a los detectores consiste en producir rutinas auto encriptadoras pero con una "llave variable". La técnica polimórfica o

"mutante" es muy sofisticada y demanda mucho conocimiento, ingenio y trabajo de programación tal como se puede apreciar en el código fuente del virus DARK AVENGER. Sin embargo existe uno de los más ingeniosos generadores automáticos de virus, llamado "Mutation Engine" (distribuido gratuitamente en Internet), que emplea un polimorfismo en la forma de módulo objeto. Con este generador, cualquier virus puede convertirse en polimórfico al agregarle ciertas llamadas a su código assembler y "enlazándolas" al Mutation Engine, por medio de un generador de números aleatorios. Los objetivos de ataque pueden ser el Boot, archivos COM o EXE y cualquier área vital del sistema, especialmente el MBR, ya sea individualmente, en forma combinada o en su totalidad. Este estilo de programación también emplea el control de memoria dinámica así como algoritmos de compresión y decomprensión de datos. Estos virus son también llamados "mutantes" . Los virus polimórficos trabajan de la siguiente manera: Se ocultan en un archivo y se cargan en memoria cuando el archivo infectado es ejecutado. Pero a diferencia de hacer una copia exacta de sí mismos cuando infectan otro archivo, modifican esa copia para verse diferente cada vez que infectan un nuevo archivo. Valiéndose de estos "motores de mutación", los virus polimórficos pueden generar miles de copias diferentes de sí mismos. A causa de esto, los rastreadores convencionales han fallado en la detección de los mismos. Ciertamente, cada rastreador de virus creado antes de Enero de 1992 no será capaz de detectar virus polimórficos. De hecho, la mayoría de las herramientas de rastreo utilizadas actualmente todavía no pueden detectar estos virus. La tecnología de Trend es una de las pocas capaz de detectar en forma consistente este tipo de virus. La tecnología de Trend puede detectar virus polimórficos observando eventos característicos que los mismos deben realizar para sobrevivir y expandirse. Cualquier virus, sin importar sus características debe hacer ciertas cosas para sobrevivir. Por ejemplo, debe infectar otros archivos y residir en memoria. Los sistemas de monitoreo de virus de Trend (como el PC-cillin, fue el primero en aplicarlo) observan estos comportamientos. Los virus polimórficos de computadora se diseñan para hacer difícil su detección, si bien los programas antivirus pueden detectar y eliminar fácilmente este tipo de virus. Los autores de los virus polimórficos encriptan el cuerpo del virus y la rutina de desencriptación. No existen dos infecciones iguales, de modo que no puede crearse una sola definición antivirus para eliminar todos los virus. Los fabricantes de soluciones antivirus usan su tecnología de protección antivirus para crear rutinas genéricas de desencriptación que dejan al descubierto el virus.

- ✓ VIRUS DE JAVA: Infectan la máquina virtual Java, que es la que se encarga de ejecutar este tipo de programas, de hay, lo que advierten siempre de desactivar esto del navegador de Internet. En 1991 Sun Microsystems, empezó a desarrollar un proyecto de lenguaje, con el código GREEN, bajo la dirección de James Goslin, inicialmente con el propósito de administrar y controlar interactivamente los dispositivos conectados a las redes. Surgieron algunas situaciones frustrantes, pero por suerte, en pocos años se empezó a popularizar Internet. Entonces el proyecto se convirtió en un intento de resolver simultáneamente, todos los problemas que se le planteaban a los desarrolladores de software por la diversidad de arquitecturas incompatibles, los sistemas operativos y lenguajes de programación y la dificultad de crear aplicaciones distribuidas en Internet. Java fue inicialmente desarrollado en C++, pero paulatinamente se fue independizando, escribiendo su propio lenguaje denominado Oak, que finalmente terminó convirtiéndose en Java. El 23 de Mayo de 1995 fue lanzado al mercado el HotJava Browser, y ese mismo año Netscape decidió habilitar a Java en su versión 2.0 de 1996. Es a partir de esa oportunidad que Java empezó a popularizarse en todo el mundo. Las características más importantes de Java son:
    1. Es de arquitectura portable, neutral y robusta.
    2. Es simple, orientada a objeto y muy versátil.
    3. Es interpretado.

El intérprete Java (System run-time) puede ejecutar directamente el código objeto. Un Applet de Java es un programa dinámico e interactivo que puede ser ejecutado dentro de un archivo HTML y mostrado por un navegador con capacidad Java. Un programa Java puede ser ejecutado por sí mismo. En todos los casos, bajo una jerarquía de Clase, Sub-Clase o Super Clase. Con todas estas características de un poderoso lenguaje, los creadores de virus pensaron también en Java, como un medio para producir especies virales. Debido a ciertas restricciones definidas en las propiedades de seguridad, tanto de los sistemas operativos, así como de los navegadores, hasta la fecha existen solamente 2 virus de Java notables:

- *Java.Beanhive* La tecnología empleada en este virus tiene varias ventajas. La forma multi componente de infección permite al virus esconder su código en los archivos infectados: su longitud crece en muy pequeños valores y después de una ligera observación el código insertado pareciera no ser dañino. La combinación del llamado starter-main también le permite a su autor, "actualizar" el virus con nuevas versiones al reemplazar el código principal en su servidor. Cabe mencionar que este virus o cualquier virus de Java se puede propagar y reproducir en condiciones limitadas. La protección estándar de seguridad de los navegadores cancela cualquier intento de acceder a las unidades de disco y hacer download de archivos como una aplicación Java, aún en modo remoto. Consecuentemente el virus puede ser propagado únicamente cuando es ejecutado en un archivo de disco, como una aplicación Java, al usar el Java machine.

  Detalles Técnicos El ejecutor del virus es un pequeño programa Java de apenas 40 líneas de código, que cuando toma el control de un sistema, se conecta al servidor WEB remoto, envía (download) el código del virus que es guardado en el archivo BeanHive.class y se ejecuta como una sub-rutina. El código viral está dividido en 6 partes y es almacenado en 6 diferentes archivos Java:

  BeanHive.class : búsqueda de archivos en un árbol de directorio
  +--- e89a763c.class : analiza el formateo de archivo
  |--- a98b34f2.class : acceso a las funciones del archivo
  |--- be93a29f.class : preparación para la infección (parte 1)
  |--- c8f67b45.class : preparación para la infección (parte 2)
  +--- dc98e742.class : insertado del virus en el sistema infectado

  Al infectar el virus, analiza los formatos internos de Java, escribe en el archivo el código de inicio como una sub-rutina "loadClass" y agrega al archivo constructor de códigos, la invocación para su sub-rutina loadClass "BeanHive". El parámetro enviado "BeanHive" apunta al nombre del archivo remoto en el servidor WEB y empieza la infección con su código viral.
- *Java.StarngeBrew*Este es el primer virus conocido que infecta archivos Java Classes. Fue reportado en Agosto de 1998 y tiene la capacidad de auto copiarse únicamente en el caso de que el acceso a unidades de disco esté permitido en las Propiedades del navegador y el sistema operativo. El archivo infectado se ejecuta como una aplicación nativa de Java y no como un Applet. Las últimas versiones de los navegadores Netsacape o IE5 emiten un mensaje de advertencia e impiden su ejecución. Si el virus es ejecutado como una aplicación, tiene la posibilidad de invocar las funciones de disco de Java, tales como: búsqueda de archivos, lectura, escritura y cierre. Al hacer uso de estas funciones, el virus ejecuta sus archivos buscando e infectando sub-rutinas (puede buscar en el directorio actual los Java Classes, e infectarlos) y al hacerlo, el virus abre los archivos en forma de información binaria, lee los encabezados y disfraza el formato interno de Java. Antes de ejecutar su rutina de infección, el virus tiene que acceder a su propio código viral, lo cual es necesario, ya que debe copiar su código a otros archivos Java, para lograr infectarlos. Este virus no está capacitado para activar su código en memoria, debido a que no existe tal función en el lenguaje Java, de tal modo que busca su propio código en el directorio vigente, analiza y disfraza su formato, busca el código viral y lo lee. Inmediatamente el virus busca otros Java Classes (que tienen la extensión .CLASS), las analiza, escribe su código en el archivo a infectar e inserta una llamada a la función principal del virus hacia la rutina principal Class. La razón del nombre de este virus se debe a que tiene la función Strange_Brew_Virus. La cadena de esta especie es visible cuando es examinada con cualquier editor de texto. Java, aplicado en archivos HTML para páginas web, es sumamente potente y puede lograr los efectos muy complejos que no podrían producirse en otro lenguaje de programación. Observe el logo flotante de S.O.S. Virus!! o haga clic en Dinamita, para visualizar un inofensivo efecto gráfico desarrollado en Java."

8.5 No son virus *CABALLOS DE TROYA o TROYANOS*: Los caballos de Troya toman su nombre del mítico caballo de Troya construido con fines bélicos que, bajo un aspecto benigno, en lo que parecía una ofrenda, escondía en su interior a un grupo de guerreros griegos.

Oculto en un programa, permite a otro usuario controlar nuestro computador desde otro lado de la Red. Los más conocidos son BACK ORIFFICE o NET BUS. Los programas diseñados con fines de devastación son una especie por sí misma: los caballos de Troya, o simplemente "troyanos". El autor del troyano no está interesado en infectar nada, sino en destruir. Por esa razón, hasta el advenimiento de la Internet, no se habían propagado de modo importante; la intensificación de un medio casi ideal para propagar lo que se desee como es el correo electrónico, ha favorecido claramente el renacimiento de una plaga que no era significativa. Como en el caso del poema homérico del que reciben su nombre los troyanos, no es el enemigo quien introduce el funesto dispositivo al sistema del usuario, sino el propio usuario, que difícilmente puede llamarse víctima después de ejecutar un programa de procedencia desconocida y, lo que es peor: sin una buena razón para hacerlo. No se trata aquí del mismo caso de los virus, porque un virus puede venir de una fuente confiable y oculto en un programa legítimo, sin conocimiento del usuario; el troyano nunca viene en un archivo legítimo, nunca hay una razón válida para ejecutarlo. Quien ejecuta un troyano lo hace asumiendo un riesgo que podía haberse evitado con solo verificar la procedencia del programa, más aun si se considera que nadie solicita un troyano. Es conveniente enfatizar la diferencia operativa de virus y troyanos: ningún programa bien intencionado tiene porqué modificar otros programas, por eso un virus puede ser identificado, porque ejecuta operaciones únicas de su naturaleza que no se encuentran en otros programas, es decir, usan una tecnología que los hace inconfundibles. Pero el troyano hace cosas que son legítimas en muchas aplicaciones: borrar archivos, formatear discos, copiar sectores, etc. En otras palabras, al troyano no lo distingue su tecnología, sino las intenciones de su autor. Y no hay forma de detectar las intenciones de un programador hasta que se aprecian los resultados de su obra. Un virus tiene diversas formas de infectar, pero todas redundan en lo mismo: se valen de un huésped al que invaden y su erradicación se limita a descontaminar el huésped o borrarlo si ha quedado inutilizable. Pero los troyanos no se pueden descontaminar porque no infectan, y no suele bastar con borrar un archivo, porque varios de los troyanos contemporáneos emplean un proceso de instalación relativamente complejo y único de cada caso, que hace imposible para un antivirus aplicar las técnicas habituales a situaciones de naturaleza completamente distinta. No hay vacunas para los troyanos, eso es un hecho. En una analogía tomada del lado humano, se puede decir que todos estamos expuestos a contraer una enfermedad viral por simple contagio ambiental, y podemos curarnos con medicinas apropiadas y aun prevenir futuras infecciones con la vacuna adecuada si la hubiera. Pero no hay vacunas que prevengan un atropellamiento en la vía pública o el ataque de una pandilla de vándalos; tampoco bastan las medicinas para recuperarnos de semejante incidente. Para evitar ese tipo de situaciones solo una cosa puede hacerse: usar el sentido común para no exponerse a riesgos innecesarios. Para concluir, debe considerarse el aspecto de la recuperación. En la mayoría de los casos, un antivirus puede ayudar a recuperarse de la infección viral a través de la descontaminación y reparación de los archivos, pero un troyano se asegura de destruir programas y datos hasta el punto de hacer imposible la recuperación

8.6 Bombas y Bombas Ansy son instrucciones para la ejecución de programas en fechas u hora determinando, para ello utilizan el reloj del sistema o por combinaciones de pulsación de teclas, que hacen que se active el disparador, tras un número determinado de ejecuciones. Una bomba lógica es un programa o parte de un programa que se ejecuta condicionalmente, dependiendo del estado de determinadas variables ambientales, causando daños al sistema donde reside o impidiendo el correcto funcionamiento del mismo. Las variables ambientales por las que puede *explotar* una bomba lógica pueden ser de muy diverso tipo, como la presencia de ciertos archivos o la realización de determinadas acciones, aunque las más comunes tienen que ver con el tiempo (fecha y hora). A este tipo se les denomina también bombas de tiempo. Las bombas lógicas son una de las amenazas software o programas malignos más antiguos que hay, anterior a los virus. Por lo general, y aunque existen algunos virus que se activan en fechas concretas, las bombas lógicas suelen ser producto de empleados descontentos o insatisfechos que programan sus sistemas de modo que son los únicos capaces de hacer que sigan funcionando, desactivando regularmente la bomba lógica. Naturalmente, en caso de ser despedidos nadie desactiva la bomba, y esta provoca los daños previstos, que como ya se ha dicho pueden oscilar entre la destrucción de todos los datos de la empresa o simplemente el bloqueo de uno o varios programas fundamentales. Otra forma que tiene el empleado descontento de conseguir sus objetivos es usando una bomba lógica que no explote en una fecha concreta, sino que explote cuando el identificador del empleado no aparezca en dos cálculos consecutivos de la

nómina. De esta manera se evita el tener que desactivarla cada cierto tiempo, evitando el riesgo de que la bomba explote por descuido. Otro tipo de bombas lógicas son fragmentos de código que algunos programadores colocan en sus programas a medida para asegurarse el cobro del trabajo. Si llegada cierta fecha el trabajo no está pagado, la bomba lógica no deja arrancar el programa, o ciertos módulos del mismo, y obviamente el programador se negará a efectuar cualquier trabajo de mantenimiento mientras no se le pague lo estipulado en un principio. Si el pago se ha realizado sin problemas, el programador, con la excusa de haber descubierto defectos o haber mejorado ciertas características, cambia la copia defectuosa por otra correcta. Por supuesto, el cliente nunca está al corriente de todo esto. Como vemos, las bombas lógicas son muy versátiles, ya que se trata de una amenaza que no actúa de forma indiscriminada, al contrario, su ejecución suele estar muy planeada y cuidada así como tener una finalidad muy específica. Es normal que la gente se confunda entre los virus con temporizador y las bombas lógicas. Sin embargo, los virus son pequeños programas que se auto reproducen infectando a otros programas y extendiéndose así de sistema en sistema, mientras que una bomba lógica no se puede reproducir, permanece como una mina en el sistema en el que fue instalada por su programador.

7 **WORNS o GUSANOS**: Se les llama a los que se multiplican y reproducen masivamente, aunque no suelen ser destructivos si son muy perjudiciales por el efecto de colapso producido, normalmente introducidos en archivos de Word o Excel. Ejemplo VBS.Bubbleboy. El primer ciber terrorista llevado a rendir cuentas ante la justicia no fue un autor de virus, ni siquiera fue un autor de troyanos, fue un joven estadounidense que alcanzó fama por haber creado un nuevo tipo de programa que se valía del correo electrónico para propagarse. Ese fue el primer gusano, o al menos fue el primero que alcanzó su meta: estrangular la supercarretera de la información saturándola de mensajes. Los gusanos, como los virus, pueden o no causar daños, pero su característica distintiva es el hecho de que se propagan a través de correo electrónico. El gusano suele ser un programa que llega anexo en un mensaje y que al ejecutarse localiza la libreta de direcciones electrónicas del usuario y envía copias de sí mismo a quienes estén registrados en el directorio electrónico. Cualquier cosa adicional que el gusano haga es independiente de su mecanismo de propagación, pudiendo ocurrir que un gusano sea también un troyano, tal es el caso del Explore_Zip, que se infiltra a las redes usando sus características de gusano, pero una vez que se introduce, emplea su faceta de troyano para infiltrar hasta los nodos de la red que no tienen correo electrónico. También hay virus agusanados. El popular virus Melissa consiguió un nivel de propagación espectacular gracias precisamente a que poseía mecanismos típicos de los gusanos para exponenciar su difusión. Ya que los gusanos contienen rutinas muy especializadas para tomar control de los recursos del correo electrónico, hasta ahora su detección no ha representado mayor problema para los antivirus, pero debido a que los gusanos pueden emplear técnicas complejas de instalación -tal es el caso del gusano "Happy99"- no es práctico para un antivirus intentar su eliminación. Como en el escenario de los troyanos, los gusanos deben ser eliminados a base de procedimientos que son como trajes hechos sobre medida: según sea el caso. No hay mejor protección contra los gusanos que la prudencia y la precaución en el manejo de archivos anexos de correo electrónico por parte del usuario

8 Trapdoor el más antiguo de los recursos de asalto a la seguridad informática sigue siendo trapdoor. Diseñadas originalmente como respuesta a la necesidad de mantener la vía de acceso a la información en sistemas de alta seguridad para casos de extravío de contraseñas o de errores en el sistema operativo, las trapdoor han existido desde siempre, es solo que no se documentan para evitar el mal uso de esa posibilidad, ya que anularía el esquema de protección que brinda el uso de contraseñas y niveles de seguridad. Puesto que las trapdoor del fabricante rara vez trascienden, ya que son secretos celosamente guardados por los autores de los programas y sistemas operativos para ser usados solo en emergencias, no cabe esperar que las trapdoor "oficiales" sean del dominio público. Pero todos los sistemas operativos tienen, invariablemente, fallas de seguridad que ni los propios desarrolladores conocen. Esas son las trapdoor "no oficiales" y son explotadas por las agrupaciones subterráneas de programadores para desarrollar herramientas que permiten infiltrar y sabotear sistemas operativos remotos. A diferencia de los troyanos, las trapdoor por lo general no incluyen código destructivo, sino que "entregan" el control del sistema infiltrado a un cliente subrepticio y anónimo para que sea éste quien haga lo que le apetezca en tiempo real. Lamentablemente en tiempos recientes se han diseminado de manera irresponsable poderosas herramientas que no solo hacen las delicias de los aprendices de Hackers, sino que proporcionan los medios

para que programadores avanzados y desprovistos de escrúpulos desarrollen a su vez herramientas de asalto sin precedente. Las trapdoor, como los troyanos, no llegan por sorpresa, se instalan porque el usuario, sin tomar las precauciones necesarias, ejecuta programas de procedencia indeterminada. Este tipo de programas tampoco es sencillo de manejar por un antivirus ya que no infecta ni contiene rutinas destructoras que permitan identificarlo en base a su contenido. Para agravar la situación, las trapdoor son programas generalmente preparados a base de un compilador cuyos ejecutables contienen bloques de código muy parecidos a los de cualquier programa convencional, de modo que tampoco es tarea simple dar con cadenas de bytes que permitan su identificación única como ocurre con los virus. Las trapdoor más difundidas como son Back Orifice y NetBus están incorporadas en algunos programas legítimos que se comercializan pública y abiertamente; suelen venir en programas de comunicaciones, servidores de fax, monitores de red y otros más que contribuyen a dificultar la distinción entre aplicaciones seguras y aquellas que ocultan aviesas intenciones. Esto significa que aun si un antivirus le reporta la presencia de una puerta trasera en una aplicación que usted compró e instaló, eso no implica que alguien pretenda infiltrar su sistema y perjudicarlo, significa solo que existe esa posibilidad.

9 Nuckers Una categoría más, poco conocida, pero no nueva ni rara, es la de los nuckers .Se trata del tipo de software más siniestro y cobarde que se haya creado. El nucker es un programa diseñado para la muerte súbita, el ataque por sorpresa, alevoso porque explota las debilidades de los sistemas operativos y de la seguridad en las redes. No hay arma ni defensa alguna que valga o prevenga el ataque de un nucker salvo, quizá, los firewalls. Aun en ese caso, pueden quedar protegidos los nodos tras el Firewall, pero el Firewall mismo está a merced de un aniquilador diduro específicamente contra él. Los nuckers se distinguen de los troyanos en dos aspectos: no vienen en archivos que el usuario ejecuta, sino que son programas ejecutados desde sitios distantes por saboteadores, por esa razón no pueden ser detectados ni removidos por la víctima; la segunda diferencia consiste en que el troyano por lo general está diseñado para destruir información y archivos de todo tipo, el aniquilador en cambio está diseñado para cortar repentinamente el funcionamiento de la máquina atacada. Esto no siempre implica la destrucción de la información, sino la paralización del sistema. Un ejemplo ya clásico es el "Ping o'Dead", un programa que ejecuta llamadas interminables a una dirección de red cualquiera hasta que la red se desquicia por saturación y falla. La máquina queda fuera de la red y se suspende todo proceso que dependa de ella. Ya que existen múltiples sites en Internet que irresponsablemente ponen nuckers de todo tipo a disposición de quien desee tomarlos, la posibilidad de sufrir un ataque de esta naturaleza está siempre latente, solo se requiere alguien decidido a "pasar un rato divertido" para sabotear incluso las redes más protegidas

10 Características de los Virus. El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo. Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huésped es cerrado. os virus pueden llegar a "camuflarse" y esconderse para evitar la detección y reparación. Como lo hacen:

a) El virus re-orienta la lectura del disco para evitar ser detectado;
b) Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus;
c) Encriptamiento: el virus se encripta en símbolos sin sentido para no ser detectado, pero para destruir o replicarse **DEBE** desencriptarse siendo entonces detectable;
d) Polimorfismo: mutan cambiando segmentos del código para parecer distintos en cada "nueva generación", lo que los hace muy difíciles de detectar y destruir;
e) Trigger se relaciona con un evento que puede ser el cambio de fecha, una determinada combinación de tecleo; un macro o la apertura de un programa asociado al virus (Troyanos).

Los virus se transportan a través de programas tomados de BBS (Bulletin Boards) o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: downloads de programas de lugares inseguros; e-mail con "attachments", archivos de MS-Word y MS-Excel con macros. Inclusive ya existen virus que se distribuyen

con MS-Power Point. Los archivos de datos, texto o Html **NO PUEDEN** contener virus, aunque pueden ser dañados por estos. Los virus de sectores de "booteo" se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de los drivers de la PC. Pueden dañar el sector o sobre escribirlo. Lamentablemente obligan al formateo del disco del drive infectado. Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M.En cambio los virus de programa, se manifiestan cuando la aplicación infectada es ejecutada, el virus se activa y se carga en la memoria, infectando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos o permanecer inactivos por largos periodos de tiempo.

11 Daños de los Virus. Definiremos **daño** como una acción indeseada, y los clasificaremos según la cantidad de tiempo necesaria para reparar dichos daños. Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad.

- ✓ DAÑOS TRIVIALES. Sirva como ejemplo la forma de trabajo del virus FORM (el más común): En el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep. Deshacerse del virus implica, generalmente, segundos o minutos.
- ✓ DAÑOS MENORES. Un buen ejemplo de este tipo de daño es el JERUSALEM. Este virus borra, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos. Esto nos llevará alrededor de 30 minutos.
- ✓ DAÑOS MODERADOS. Cuando un virus formatea el disco duro, mezcla los componentes de la FAT (File Allocation Table), o sobrescribe el disco duro. En este caso, sabremos inmediatamente qué es lo que está sucediendo, y podremos reinstalar el sistema operativo y utilizar el último backup.
- ✓ DAÑOS MAYORES. Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un backup volvamos al último estado de los datos. Un ejemplo de esto es el virus DARK AVENGER, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: "Eddie lives ... somewhere in time" .Esto puede haber estado pasando por un largo tiempo sin que lo notemos, pero el día en que detectemos la presencia del virus y queramos restaurar el último backup notaremos que también él contiene sectores con la frase, y también los backups anteriores a ese. Puede que lleguemos a encontrar un backup limpio, pero será tan viejo que muy probablemente hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad a ese backup.
- ✓ DAÑOS SEVEROS. Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del DARK AVENGER (es decir, no podemos buscar la frase Eddie lives)
- ✓ DAÑOS ILIMITADOS. Algunos programas como CHEEBA, VACSINA.44.LOGIN y GP1 entre otros, obtienen la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos no son virus sino troyanos. En el caso de CHEEBA, crea un nuevo usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que quisiera.

12 Síntomas Típicos de una Infección. Los síntomas más comunes que caben esperarse son:

- ❖ El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
- ❖ El tamaño del programa cambia sin razón aparente.
- ❖ El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.
- ❖ Si se corre el CHKDSK no muestra "655360 bytes available".
- ❖ En Windows aparece "32 bit error".
- ❖ La luz del disco duro en la CPU continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- ❖ No se puede "bootear" desde el Drive A, ni siquiera con los discos de rescate.
- ❖ Aparecen archivos de la nada o con nombres y extensiones extrañas.

- Suena "clic" en el teclado (este sonido es particularmente aterrador para quien no esta advertido).
- Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).
- En la pantalla del monitor pueden aparecen mensajes absurdos tales como **"Tengo hambre. Introduce un Big Mac en el Drive A".**
- En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrios repartidos de colores y una leyenda en negro que dice Windows '98 (No puedo evitarlo, es mas fuerte que yo...!!).

Una infección se soluciona con las llamadas "vacunas" (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados. Hay cierto tipo de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infectado.

13 ¿Qué es un Antivirus?. para toda enfermedad no existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes. Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no sólo no será eficaz para el 100% de los casos, sino que nunca será una protección total ni definitiva. La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada. El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue utilizando (aunque cada vez con menos eficiencia), es la técnica de scanning. Esta técnica consiste en revisar el código de todos los archivos contenidos en la unidad de almacenamiento -fundamentalmente los archivos ejecutables- en busca de pequeñas porciones de código que puedan pertenecer a un virus informático. Este procedimiento, denominado escaneo, se realiza a partir de una base de datos que contiene trozos de código representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda. La técnica de scanning fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo. El primer punto grave de este sistema radica en que siempre brinda una solución *a posteriori*: es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado. Además, este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva), que deben actualizarse periódicamente debido a la aparición de nuevos virus. En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades.

En virtud del pronto agotamiento técnico de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados. Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que

presenta este tipo de algoritmo radica en **que puede llegar a sospecharse de duchísimas cosas que no son virus**. Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico. Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan **chequeadores de integridad**. Sobre la base de estas consideraciones, podemos consignar que **un buen sistema antivirus** debe estar compuesto por **un programa detector de virus** -que siempre esté residente en memoria- y **un programa que verifique la integridad** de los sectores críticos del disco duro y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

14 Modelo de Antivirus. La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado de control y el segundo denominado de respuesta. A su vez, cada uno de ellos se divide en varias partes:

1) **Módulo de control:** posee la técnica **verificación de integridad** que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco duro. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco duro que no son modificados a menos que el usuario lo requiera. Otra opción dentro de este módulo es la **identificación de virus**, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos. Asimismo, la **identificación de código dañino** es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco duro. Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas. Finalmente, el módulo de control también posee una **administración de recursos** para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a disco, etc.). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.
2) **Módulo de respuesta:** la función **alarma** se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla. Algunos programas antivirus ofrecen, una vez detectado un virus informático, la posibilidad de erradicarlo. Por consiguiente, la función **reparar** se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada. Por otra parte, existen dos **técnicas para evitar el contagio de entidades ejecutables**: evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.
   Aunque la primera opción es la más adecuada, plantea grandes problemas de implementación.

15 Detección y Prevención. Debido a que los virus informáticos son cada vez más sofisticados, hoy en día es difícil sospechar su presencia a través de síntomas como la pérdida de Performance. De todas maneras la siguiente es una lista de síntomas que pueden observarse en una computadora de la que se sospeche esté infectada por alguno de los virus más comunes:

- Operaciones de procesamiento más lentas.
- Los programas tardan más tiempo en cargarse.
- Los programas comienzan a acceder por momentos a las disco de arranques y/o al disco duro.
- Disminución no justificada del espacio disponible en el disco duro y de la memoria RAM disponible, en forma constante o repentina.
- Aparición de programas residentes en memoria desconocidos.

La primera medida de prevención a ser tenida en cuenta es, como se dijo anteriormente, contar con un sistema antivirus y utilizarlo correctamente. Por lo tanto, la única forma de que se constituya un bloqueo

eficaz para un virus es que se utilice con determinadas normas y procedimientos. Estas normas tienden a controlar la entrada de archivos al disco duro de la computadora, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y, por supuesto, disminuyendo al mínimo posible todo tipo de tráfico. Además de utilizar un sistema antivirus y controlar el tráfico de archivos al disco duro, una forma bastante eficaz de **proteger los archivos ejecutables** es utilizar un programa **chequeador de integridad** que verifique que estos archivos no sean modificados, es decir, que mantengan su estructura. De esta manera, antes que puedan ser infectados por un virus convencional, se impediría su accionar. Para prevenir la infección con un **virus de sector de arranque**, lo más indicado es no dejar disquetes olvidados en el disco "a" de arranque y contar con un antivirus. Pero, además, puede aprovecharse una característica que incorpora el setup de las computadoras más modernas: variar la secuencia de arranque de la PC a **"primero disco duro y luego disco "a"** (C, A). De esta manera, la computadora no intentará leer el disco de arranque aunque tenga cargado un disquete. En consecuencia, la detección alternativa a la de scanning y las de chequeo de actividad e integridad resultan importantes, ya que pueden detectar la presencia de un virus informático sin la necesidad de identificarlo. Y esta es la única forma disponible para el usuario de detectar virus nuevos, sean nacionales o extranjeros. De todas maneras, **existe una forma de actualizar la técnica de scanning**. La misma consiste en incorporarle al antivirus un archivo conteniendo cadenas de caracteres ASCII que sean trozos de código (strings) significativos del sector vital de cada nuevo virus que todavía no esté incorporado en la base de datos del programa.De todas formas, esta solución será **parcial**: la nueva cadena introducida sólo *identificará* al virus, pero no será capaz de erradicarlo. Es muy importante que los "strings" que se vayan a incorporar al antivirus provengan de una fuente confiable ya que, de lo contrario, pueden producirse falsas alarmas o ser ineficaces.
La NCSA (National Computer Security Association, Asociación Nacional de Seguridad de Computadoras) es la encargada de certificar productor antivirus. Para obtener dicha certificación los productos deben pasar una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario. Antiguamente el esquema de certificación requería que se detectara (incluyendo el número de versión) el 90 % de la librería de virus del NCSA, y fue diseñado para asegurar óptimas capacidades de detección. Pero esta metodología no era completamente eficiente. Actualmente, el esquema de certificación enfoca la amenaza a las computadoras empresariales. Para ser certificado, el producto debe pasar las siguientes pruebas:

a) Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.
b) Deben detectar, como mínimo, el 90% de la librería de virus del NCSA (más de 6.000 virus)

Estas pruebas son realizadas con el producto ejecutándose con su configuración "por defecto". Una vez que un producto ha sido certificado, la NCSA tratará de certificar nuevamente el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación. Si un producto no pasa la primera o segunda prueba, su distribuidor tendrá siete días para proveer de la corrección. Si este límite de tiempo es excedido, el producto será eliminado de la lista de productos certificados. Una vez que se ha retirado la certificación a un producto la única forma de recuperarla es que el distribuidor envíe una nueva versión completa y certificable. Acerca de la lista de virus de la NCSA, aclaremos que ningún desarrollador de antivirus puede obtener una copia. Cuando un antivirus falla en la detección de algún virus incluido en la lista, una cadena identificadora del virus le es enviada al productor del antivirus para su inclusión en futuras versiones. En el caso de los virus polimórficos, se incluyen múltiples copias del virus para asegurar que el producto probado lo detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.
La A. V. P. D. (Antivirus Product Developers, Desarrolladores de Productos Antivirus) es una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

- Cheyenne Software
- I. B. M.
- Intel
- McAfee Associates
- ON Technology
- Stiller Research Inc.
- S&S International

- Symantec Corp.
- Thunder Byte

Anexo 9

Sistemas Operativos

1 Windows NT

1.1 Antecedentes Windows NT fue desarrollado para convertirse en un sistema operativo para correr aplicaciones críticas. Creado por Microsoft como competencia del sistema operativo UNIX, agregando un alto nivel de Seguridad. Fue diseñado por Dave Cutler, el mismo diseñador del sistema operativo VMS. A través del equipó de desarrollo de Windows NT, se combinaron aspectos de un microkernel (una variante de UNIX desarrollada en la Universidad de Carnegie-Melon) y VMS para desarrollar Windows NT.

1.2 Seguridad C2 La seguridad en Windows NT se basa en las reglas de seguridad propuestas por el departamento de defensa de los Estados Unidos y publicado en Diciembre de 1985 en un documento denominado "Trusted Computer System Evaluation Criteria". Este nivel de seguridad denominado C2 aplica solamente a las estaciones de trabajo, por lo cual no incluye la seguridad en Red. Aunque no incluye la seguridad de red en general, proveen a un sistema un alto nivel de seguridad y un paso necesario para este tipo de seguridad. Entre las reglas que este nivel de seguridad ofrece se encuentran:

- Cada usuario debe estar identificado y autentificado usando una sola clave y contraseña, y toda actividad de usuarios debe ser registrado usando esta identificación.
- Los recursos deben tener propietarios que se encarguen de controlar el acceso a estos recursos.
- Los objetos deben estar protegidos a que otros procesos o usuarios utilicen, permitiendo restringir su uso. Esta protección aplica a las localizaciones de memoria, archivos y otros objetos.
- Cualquier evento de seguridad debe ser auditado y los datos obtenidos a partir de la auditoria deben estar restringido a los usuarios no autorizados.
- El sistema puede protegerse de interferencia o manipulación externa tal como modificaciones al sistema de arranque o al sistema de archivos.

Windows NT, aparte de implementar estas reglas, ofrece otro conjunto de reglas que fortalecen el sistema de seguridad. Entre estas se encuentran:

- Control de accesos a recursos, archivos, carpetas, servidores, impresoras y aplicaciones.
- Gestión de cuentas de usuarios así como bloqueo de cuentas.
- Asignación de recursos a usuarios y capacidad para definir el acceso a estos recursos.
- Asignación de operaciones sobre contraseñas.
- Vencimientos de contraseñas.
- Ofrece un nivel de encriptación que previene la obtención de contraseñas a través de la red "Sniffing".

1.3 Estructura de Windows NT, la arquitectura de Windows NT esta conformado por los siguientes elementos

Kernel: es un pequeño programa que permite interactuar con cada uno de los procesadores del mercado. Por ejemplo. Linux posee un Kernel diferente para cada arquitectura diferente. También se encarga de sincronizar las actividades de los componentes de los módulos superiores.

Hardware Abstraction Layer (HAL): Permite facilitar la labor de los programadores, ya que sirve como una interfaz abstracta entre los dispositivos de hardware y las capas superiores.

Object Manager: Archivos, carpetas, puertos, procesos, e hilos son denominados objetos. Este se encarga de localizar y disponer los objetos

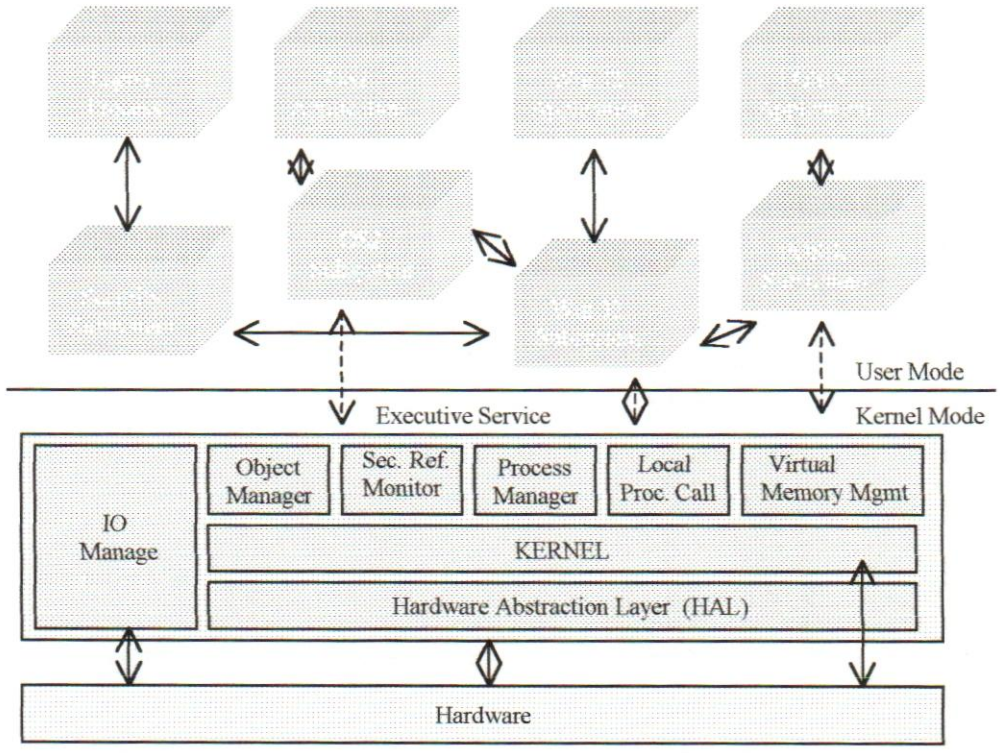
Process Manager: Un componente que crea y elimina procesos

Virtual Memory Manager: Es el componente que crea memoria simulada en el disco duro.

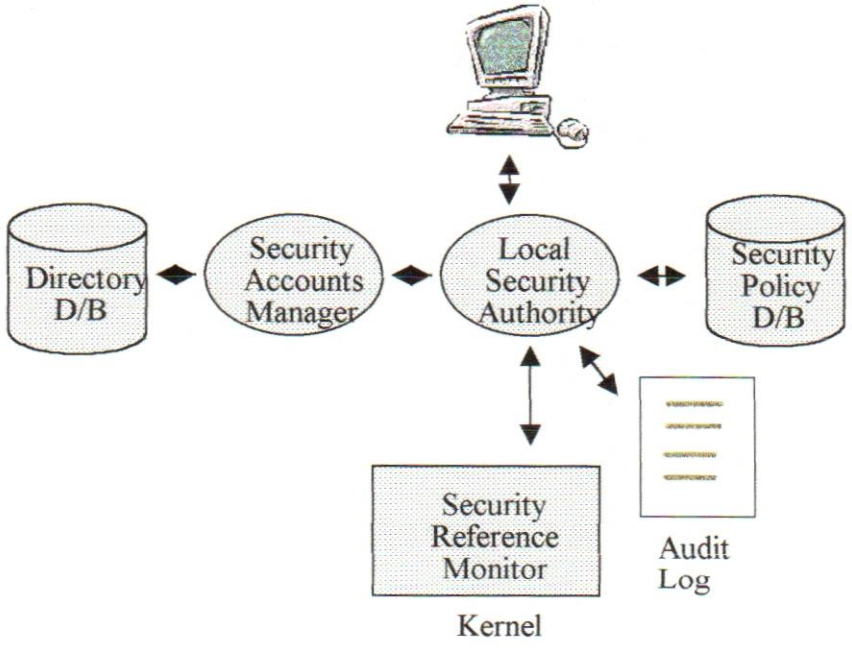
Local Procedure Call Facility: Este módulo es utilizado por las aplicaciones para comunicarse con niveles inferiores del sistema operativo vía mensajes.

I/O Manager: Es un componente que administra la comunicación entre el sistema operativo y el mundo externo. Este maneja Configuración de dispositivos el cual son módulos de software que ayuda al sistema operativo acceder a dispositivos físicos como Tarjetas de red, unidades de discos, etc.

La Arquitectura se representa en la siguiente figura



El Subsistema de Seguridad en Windows NT



1.4 Subsistema de seguridad en Windows NT El subsistema de seguridad afecta a todo Windows NT. Este provee un sistema individual el cual todos los accesos a objetos, incluyendo archivos en discos, procesos en memoria o puertos a dispositivos externos son chequeados. Esto permite que ningún usuario o aplicación pueda tener acceso sin autorización. Entre los componentes del subsistema de seguridad se encuentran:

- *Local Security Authority:* Este es el componente central del subsistema de seguridad que genera "Tokens" de acceso. También administra las políticas de seguridad en el computador local y provee autentificación para los usuarios en el proceso de "logon".
- *Logon Process:* Este proceso abre una sesión tanto en usuarios locales como en remotos.
- *Security Accounts Manager (SAM):* este sistema mantiene una base de datos de usuarios que están autorizados para acceder el sistema y verificar usuarios durante el proceso de apertura de una sesión.
- *Security Reference Monitor (SRM):* este es un componente modo Kernel, que previene acceso directo a objetos de cualquier usuario o proceso. Este valida todos los accesos a objetos.
- *Directory database:* Se encuentran almacenados la identificación de cada usuario sea localmente o remotamente.

1.4 Sistema de aperturas de sesión (logon Process) El proceso de Logon sigue los siguientes pasos

- El usuario introdúcela clave y contraseña así como el dominio el cual quiere acceder.
- El LSA corre un paquete de autentificación para validar al usuario.
- Si la sesión es local, entonces el paquete de autentificación solicita al SAM que verifique si el usuario existe en la Base de datos. En caso que exista un dominio especificado, este es enviado al computador central vía red.
- El local o dominio SAM retorna una identificación apropiada del usuario así como sus privilegios, dirección local y otros datos.
- El LSA crea un Token de acceso que contiene la identificación del usuario, el grupo a la cual pertenece y los derechos que tiene en el sistema local.
- Crea una asignación y corre el programa.

1.6 Dominios Los dominios son colecciones de computadoras y usuarios que son administrados por una autoridad central. Los dominios pueden representar departamentos, divisiones y grupos de trabajo así como otro grupo de computadoras. Su uso permite hace grupos de computadoras más manejables y para aplicar políticas de seguridad diferentes a cada área específica de la red. Los dominios proveen:

- Una cuenta de usuario individual para cada usuario.
- Un sólo proceso de apertura de sesión para acceder a cualquier recurso de la red.
- Administración centralizada de los usuarios, grupos y recursos.

1.7 Cuentas y grupos de usuarios Las cuentas de usuario contienen información sobre usuarios, tal como, su nombre, clave, contraseña, localización de su directorio raíz, información sobre cuándo y cómo el usuario puede abrir la sesión así como su configuración del escritorio.

1.7.1 Los grupos son colecciones de usuarios diseñados para compartir recursos. Se pueden dividir en dos grupos:

- *Grupos locales*: este tipo de grupo define permisos y derechos para usuarios de máquinas locales dentro de un dominio. También se puede agregar cuentas de usuarios y grupos de otros dominios a este grupo.
- *Grupos Globales*: consiste en las cuentas de usuarios pertenecientes sólo al dominio donde el grupo global fue creado. También los grupos globales pueden convertirse en miembros de un grupo global que es parte del mismo dominio o pertenecientes a otros dominios.proceso de "Log on" o apertura de sesión se muestra en la siguiente figura:

1.9 Sistema de Archivos en Windows NT La siguiente sección trata sobre la seguridad y protección de archivos y recursos de máquinas en Windows NT y cómo compartir dichos recursos con usuarios en la red de Windows. Adicionalmente, usuarios con otras versiones de Windows pueden buscar en la red por recursos compartidos de una máquina con Windows NT Server, es decir, buscar carpetas, archivos o recursos de hardware o software por medio del servidor de NT En el esquema de red de Microsoft, cualquier computadora de la red puede compartir sus recursos (directorios, archivos, impresoras, etc.), de forma tal que otros usuarios puedan acceder a dichos recursos desde cualquier punto de la red. Esto se denomina redes de punto (*peer networking*). En el modelo de redes de punto un servidor de red dedicado permite que usuarios desde sus propias estaciones compartan recursos. Muchos administradores piensan que manejar y controlar la seguridad en este tipo de arquitectura de red puede ser una pesadilla. En este caso, Windows NT Server es la única vía para hacerlo. Cada usuario posee una cuenta denominada "*User Account*" en un servidor de seguridad (*Security server*), es decir, un servidor controlador de dominios NT, y debe ser autenticado por un servidor antes de que los usuarios puedan acceder a los recursos en el servidor o en computadoras personales que tienen recursos compartidos.

1.9.1 Resource Sharing De esta forma, desde una máquina con Windows NT, se pueden otorgar permisos sobre recursos propios a usuarios específicos. Existen dos formas para realizar esto, estas dependen de que los sistemas mantengan o no una base de datos de cuentas de usuario.

- *Share-Level Access*. En este modelo, los usuarios comparten sus recursos e impresoras con cualquier otro especificando en tipo de acceso, bien sea solo de lectura (*read only*) o acceso total (*full access*), y además definiendo o no contraseña de acceso. En caso de emplear la contraseña para acceder al recurso compartido, el usuario debe pasar la clave a aquellos usuarios a los cuales les está permitiendo el acceso. Este esquema no es recomendado bajo ambientes seguros.
- *User-Level Access*. Este nivel provee una alta seguridad de control de acceso y al compartir recursos y requiere que una máquina Windows NT con la base de datos de las cuentas de seguridad sea colocada en la red para autenticar a los usuarios.

Por supuesto, máquinas con Windows NT Server son colocadas como servidores dedicados. Implementan además técnicas avanzadas de asignación de recursos y permisos a los recursos y para manejar la red completa.

1.9.2 File Allocation Table (FAT) Este es el File System utilizado en DOS, y versiones anteriores de Windows. Este tipo de File System puede ser usado en máquinas con Windows NT, pero de igual forma no es recomendado dado a que no es un sistema seguro. Mientras este sistema de archivos permita marcar archivos como ocultos o de solo lectura, cualquiera que tenga acceso a dicha máquina puede cambiar dichos permisos.

1.9.3 NT File System (NTFS) El NTFS es un sistema de archivos altamente seguro que provee vías seguras para salvaguardar información valiosa. NTFS trabaja en conjunto con el sistema de cuentas de usuario de Windows NT para autenticar usuarios cuando intentan acceder a los recursos. La seguridad y el desempeño son una de las principales características de este File System. Las opciones de seguridad en este ambiente son altamente configurables, y se acceden de manera fácil a través de ventanas por medio de las cuales se pueden configurar los recursos que se desean compartir, a qué usuarios, y con qué permisos (bien sea con o sin necesidad de una clave). Una vez se ha garantizado el acceso a un usuario, éste desde cualquier estación puede utilizar el recurso compartido siempre y cuando el usuario haya sido autenticado por sistema operativo o servidor seguro, ambos bajo ambiente de Windows NT. La seguridad provista por NTFS está basada en los controles de sistema que son manejados a través del sistema operativo de Windows NT. Una vez que el sistema operativo está montado y corriendo, los permisos NTFS y los controles de acceso a usuarios previenen de cualquier usuario que intente acceder de forma no autorizada a los archivos sobre la red. Pero si las personas pueden tener acceso físico al servidor y apagar el sistema operativo Windows NT, este pueden utilizar programas de bajo nivel que le permitan buscar volúmenes en el NTFS y leer o cambiar información de los mismos. Esta no es una posibilidad remota. Los Técnicos de Servicios usan dichos programas en casos generales para recuperar la data de unidades defectuosas. Microsoft respalda la seguridad de su File System apoyándose en la evaluación realizada al SO efectuada por el *National Computer Security Council (NCSC)*, una división de la *National Security Agency (NSA)*. El

programa C2 de evaluación de productos confiables de la NCSC provee una serie de criterios para construir y certificar sistemas operativos seguros C2. El programa de evaluación encontró que Windows NT entró en los niveles de seguridad de C2 en ciertos procesos y que sus elementos de seguridad para proteger objetos creados a bajo nivel proveen seguridad a alto nivel. El factor importante a considerar es la seguridad física del servidor de NT. Microsoft no se muestra preocupado de que Windows NT no pueda proteger información de negocios crítica cuando el servidor se encuentra apagado, por tanto los administradores necesitan asegurar físicamente todo el hardware del servidor. El uso de contraseñas para evitar el encendido no autorizado (*ROM – BIOS Setup Password*), mantener los servidores en cuartos especiales a los cuales solo usuarios autorizados pueden entrar, y prevenir que el sistema sea iniciado con un sistema operativo distinto, inhabilitar y remover o bloquear las unidades de disco son las prioridades para los administradores.

1.10 Compresión y Encriptación_ el sistema Windows NT provee otras técnicas para proteger la información almacenada en las unidades de la máquina. Elementos como la compresión de datos y el encriptamiento proveen un nivel superior de seguridad que evitaría, en caso de que la unidad de disco sea robada, que la lectura de la información sea directa, resultando esta en una traba más para el usuario no autorizado. Encriptar no siempre es una buena opción. Un Hacker que gane el acceso al servidor bien sea de forma local o a través de la red puede encriptar los archivos y bloquear totalmente al usuario o propietario de la data. Además si el usuario olvida la contraseña de encriptación no hay forma de recuperar la data de forma rápida y sencilla, por todo ello al optar por esta opción deben tomarse las precauciones del caso.

1.11 Seguridad Física La protección de archivos de NTFS solo es buena si algún usuario no puede iniciar el servidor de Windows NT utilizando DOS o por medio de otro sistema operativo como Linux. Dicha protección involucra:

- Remover o bloquear la unidad de disco flexible.
- Configurar el BIOS del servidor de forma que iniciar por medio de una unidad de disco flexible no esté habilitado y que se requieran claves para iniciar la máquina.
- No crear particiones de DOS en el servidor.
- Resguardar el sistema en un área segura.
- Configurar alarmas y/o alertas que informen cuando el servidor está caído de forma de poder detectar cuando un Hacker está en dicho proceso.

1.12 Nuevos File Systems Los últimos sistemas de archivos que han sido creados por Microsoft son los siguientes: *FAT32*. La principal diferencia entre este sistema y la versión FAT es que soporta unidades de disco de gran capacidad (hasta 2 terabytes) a diferencia del sistema FAT que solo soporta unidades de disco de 2 gigabytes. Este sistema tiene algunos problemas con algunas aplicaciones e incluso puede tener problemas con algunos antivirus debido a los cambios realizados en la estructura del sistema.

1.13 Common Internet File System (CIFS). Esta es una tecnología para compartir archivos a través del acceso remoto a la red que permite el trabajo en colaboración a través de Internet. Difiere de otros protocolos como FTP dado a que no requiere bajar los archivos de su origen para poder leer o escribir en ellos. El objetivo es mejorar el desempeño, manejar archivos de simples ubicaciones (una sola) e implementar seguridad. Algunas características son:

- El servicio de nombres de dominios (*Domain Name Service - DNS*) se emplea para ARP.
- Esta diseñado para trabajar bien sobre líneas de acceso telefónico.
- Permite a los usuarios finales trabajar en ambientes de colaboración a través de la red.
- Provee autenticación, bloqueo de archivos, compartir datos y seguridad de archivos por niveles.
- Soporta compartir impresoras a través de acceso remoto.

1.14 Administración, monitoreo y auditoria en NT Las herramientas de manejo de Windows NT permiten controlar las configuraciones, verificar el rendimiento y las actividades de los servidores y de la red. Se puede emplear estas herramientas para monitorear la seguridad de los sistemas. Las herramientas más comunes son:

- *The Windows NT Diagnostics*. Esta herramienta es muy útil para configurar y chequear los errores en el hardware del sistema y componentes Add-in.

- *The Server Manager*. Esta herramienta se emplea para controlar los servidores individuales en dominios, las conexiones de usuarios y las propiedades de los servidores.
- *The Network Monitor*. Permite capturar y ver paquetes (o más apropiadamente, Frames) en las redes. No solo se puede emplear esta herramienta para detectar problemas en la red sino además se puede emplear para monitorear actividades de Hackers en la red.
- *The Event Viewer*. Esta herramienta se emplea principalmente para ver el contenido de los archivos de LOG.

Es importante conocer estos comandos y herramientas dado a que algunos Hackers y administradores ociosos suelen usarlas para ver y cambiar información de otros sistemas, por tanto es buena idea estar familiarizado con sus armas. Como siempre, el uso de estas herramientas requiere el estado de Administrador o de Operador del directorio raíz del sistema (*systemroot/System32*). De manera general, a continuación se listan las funciones o actividades que pueden realizar en conjunto las herramientas antes mencionadas.

- Configurar alertas para detectar actividades de intrusos o intentos de acceder a archivos a los cuales no está autorizado.
- Ver información de múltiples máquinas al mismo tiempo. Es decir, se pueden ejecutar varias copias de estas herramientas para tener el control de varias máquinas a la vez y controlar los eventos que en ellas ocurren.
- Recopilar información en forma gráfica, logs, logs de alertas, y reportes para futuros análisis e impresiones.
- Configurar alertas para rastrear y comparar los valores de los contadores para:
    - Crear archivos extensos para acumular la información de los logs.
    - Guardar las configuraciones y valores actuales para futuros gráficos.

1.15 Monitoreo de la red Esta herramienta de Windows NT permite monitorear el tráfico de la red en una máquina. Solo puede ser usada para rastrear paquetes de información que son enviados o recibidos por la máquina donde se está ejecutando la aplicación. Además es una herramienta de diagnóstico para monitorear redes de área local, localizar servidores caídos, o localizar cuellos de botella. Esta herramienta muestra la siguiente información:

- Información sobre el host que envía un Frame a través de la red.
- información sobre el host que recibe el Frame.
- Los protocolos empleados para enviar el Frame.
- La data, o una porción del mensaje que ha sido enviado.

Dadas las funciones que posee esta herramienta, el Network Monitor puede ser configurado de manera de poder detectar instalaciones de si mismo y guardar la información del usuario que efectuó la instalación, de tal forma de no permitir que usuarios no autorizados puedan monitorear el tráfico de la red.

1.16 Auditoria La auditoria es crítica para mantener la seguridad de los servidores y las redes. El sistema de auditoria de Windows NT permite rastrear eventos que ocurren en servidores individuales que se relacionan con políticas de seguridad, eventos del sistema, y eventos de aplicaciones. El sistema de auditoria produce registros que pueden ser vistos con la herramienta mencionada anteriormente, The Event Viewer. Con este sistema se pueden rastrear las actividades realizadas por usuarios autorizados así como por usuarios que han ganado el acceso de forma no autorizada a través de las cuentas de otros usuarios. Existen dos tipos de auditorias que pueden ser realizadas por medio de la herramienta propia de Windows NT:

- *User Account Auditing*. Rastrea eventos de seguridad y coloca entradas en los registros de seguridad del servidor (logs).
- *File System Auditing*. Rastrea eventos del File System.

1.17 Tolerancia a fallas y protección de datos La labor de todo administrador es asegurar que la información este disponible para todos los usuarios y protegida contra la corrupción o pérdida de la misma. Los ataques de Hackers, usuarios no autorizados, o virus pueden destruir todos los planes. De la misma forma puede suceder cuando ocurren fallas debido a causas naturales. A continuación se presentan algunas técnicas de protección de la información y tolerancia a fallas.

1.17.1 Protegiendo el Sistema Operativo Un elemento importante para recuperar la información que pueda verse afectada por cualquiera de los problemas anteriores es el disco de respaldo de emergencia (*Emergency Repair Disk*). Este disco permite:

- Reparar datos dañados del registro.
- Recuperar archivos corruptos o perdidos en la partición del sistema.
- Reemplazar un *Kernel* corrupto, el cual es el centro del sistema operativo de Windows NT.
- Reemplazar sector de inicio dañados por una partición FAT.

Cuando ocurre un error, el sistema realiza lo siguiente (recuperación de errores):

- Escribe el evento en el registro de sistema (LOG).
- Envía una alerta al administrador.
- Escribe información de debug en el archivo *systemroot\MEMORY.DMP*.
- Automáticamente reinicia el sistema.

En caso de detectarse una falla cuando la máquina inicia luego de un error fatal, el sistema tiene la opción de iniciar con la última configuración correcta conocida, esto permite recobrar información que pudo haberse perdido por la instalación de componentes defectuosos que bloquearon al sistema.

1.17.2 Protegiendo el registro El sistema operativo Windows NT guarda información crítica en el registro. La seguridad de las bases de datos y la información del sistema es almacenada en archivos que se localizan en el directorio *systemroot\System32\CONFIG*. Esta información es respaldada automáticamente en el directorio *systemroot\REPAIR*. Esta información se puede actualizar manualmente en el disco de respaldo.

1.17.3 Procedimiento de recuperación de daños en el SO Cuando un error fatal ocurre, existen dos formas de recuperar la configuración del sistema, una es reinstalando el sistema operativo y otra es siguiendo un proceso de recuperación que incluye restaurar la configuración del sistema a través de un disco de respaldo. El procedimiento de respaldo es el siguiente:

- Usar dos unidades separadas en el servidor, una para el sistema operativo y otra para la data. Si el sistema operativo esta corrupto, rápidamente se puede recuperar la información en línea sin necesidad de restaurar todos los datos como tal.
- Emplear el Backup Utility para mantener conjuntos de respaldos separados para el sistema operativo y para la data. Cuando ocurre una falla en el sistema, será necesario recuperar la información del sistema operativo.
- Cada vez que se realice un cambio en la configuración del sistema, ejecutar el comando RDISK antes y después de efectuar el cambio para actualizar el disco de respaldo de emergencia. Será necesario entonces mantener dos discos con información del 'antes' y el 'después'.
- En el momento que se necesite recuperar un sistema con fallas, reiniciar el sistema y utilizar el disco de respaldo de emergencia para recuperar parte del sistema operativo. Luego reiniciar la máquina y utilizar el respaldo para recuperar la información de la partición del sistema.

1.17.4 Tolerancia a Fallas La tolerancia a fallas se refiere a la protección que posee el sistema ante fallas potenciales del hardware, desastres, infecciones de virus, ataques de Hackers, y otros riesgos. Una forma de recuperar la data es haciendo copias redundantes, usualmente en tiempo real, así como respaldos en cintas magnéticas o discos ópticos. Existen varias formas de respaldar la data:

- *Mirrored Disks (Configuración espejo)*. En esta configuración, dos discos duros (o un conjunto de discos) son utilizados, y simultáneamente la data es escrita y leída desde ambos discos. Si uno de los dos discos falla, el otro puede proveer la data a los usuarios y resulta totalmente transparente el cambio de un disco a otro.
- *Striped Sets with Parity*. En este esquema, la data es escrita sobre un arreglo de discos. La información de paridad es usada para reconstruir la data que debería estar en un disco en caso de falla.
- *Tape Backup with Off-site Archiving*. Aquí la data es copiada en múltiples conjuntos de cintas (o discos ópticos) y llevados a lugares remotos seguros para ser archivados. El método de respaldo en este caso depende de las políticas definidas.

1.17.5 Recomendaciones para el respaldo de la data Es importante tener respaldo de la información almacenada en los servidores. Existen distintos mecanismos para hacer esto. Por tanto, para cubrir los aspectos de cualquier esquema de respaldo podemos identificar acciones claves que deben realizarse en cualquiera de estos esquemas.

- Respaldar el sistema completo regularmente o cuando se realicen cambios mayores al software, a la estructura de directorios o a la configuración.
- Realizar respaldos incrementales a los archivos que han cambiado desde el último respaldo significativo. Si la información cambia constantemente entonces se deben hacer respaldos constantes.
- Guardar duplicados del respaldo en lugares apropiados, alejados lo más posible de desastres locales como incendios, terremotos o inundaciones.
- Programar todos los backups durante las horas cuando menos archivos son utilizados por los usuarios.
- Antes de poner al servidor en servicio, respaldarlo, luego intentar restaurar la información para estar seguro de que todo funciona bien y que se esta familiarizado con el proceso.

1.20 Seguridad en redes

1.20.1 Seguridad en estaciones de trabajo El sistema operativo Windows NT, provee distintas formas de ofrecer seguridad al nivel de usuario o de las estaciones de trabajo propiamente. Hemos visto que alguna de esas ventajas alcanzan niveles de seguridad C2. De esta forma podemos describir una parte de dichas herramientas de seguridad. Como se mencionó anteriormente, un método seguro de proteger la data es encriptarla, pero comentábamos también que puede tener una doble cara en caso de extraviar las claves o los algoritmos de encripción. Veamos algunas formas en las que puede ser implementada:

- *Encrypt the boot record.* Esta opción oculta las particiones del disco de modo que cualquiera que trate iniciar desde un disco flexible no pueda ver la unidad C.
- *Encrypt the System Area.* Esta opción oculta ambos, el registro de inicio (*booting*) y la FAT.
- *Partition.* Esta opción oculta el registro de inicio (*booting*), la FAT, y todos los archivos en la partición de una unidad de disco.
- *Entire drive.* Esta opción oculta la unidad completa, es decir, encripta todo su contenido.

Estas operaciones se pueden complementar con otras funciones del sistema Windows NT. Estas son algunas:

- Identificación y autenticación de usuarios.
- Elementos anti-hacking que pueden inhabilitar el sistema después de varios intentos de LOGON que fuercen al sistema a ser apagado.
- Control de acceso por puertos seriales y paralelos o lectura y escritura de discos flexibles.
- Protección transparente del inicio por medio de encriptación limita el acceso al BIOS por usuarios no autorizados.
- Integración con SECUREID Card disponible desde Secure Dynamics, proveen capacidades de autenticación duales.

1.20.2 Administración Remota Las siguientes herramientas permiten manejar y administrar la seguridad en estaciones de trabajo.

- *The System Monitor.* Esta herramienta permite monitorear el rendimiento de los sistemas en la red. Con esta herramienta el administrador puede monitorear la información que se genera por la actividad de usuarios y del File System.
- *The Net Watcher.* Si existen archivos o impresoras compartidas entre las máquinas, esta herramienta se puede utilizar para monitorear y administrar los recursos de máquinas remotas.
- *The System Policy Editor.* Esta herramienta se emplea para administrar las políticas y controlar las configuraciones de los sistemas para las máquinas en la red.
- *The Registry Editor.* Esta herramienta permite editar el registro en máquinas locales o a través de la red.

1.20.3 Manejo de Políticas y Perfiles Para un mejor control y manejo de las políticas y asignación de usuarios se deben tener en cuenta los siguientes puntos.

- Por razones de seguridad, considerar solo las políticas sobre perfiles únicos o del sistema, no de perfiles que los usuarios puedan controlar o manejar ellos mismos.
- Para un control máximo, utilizar políticas de sistema en lugar de políticas sobre usuarios únicos. Ambos requieren de un servidor en la red, de modo que los perfiles y los archivos de las políticas pueden ser almacenados fuera de la máquina del usuario, lo cual previene que el usuario los borre o modifique.
- Debe existir un directorio raíz para cada usuario en un servidor cuando se empleen ambas políticas, de sistema y de perfiles únicos.
- Usuarios indicados pueden sobrescribir políticas y perfiles, pero no se debe considerar esto una total solución de seguridad. Ese tipo de usuario está designado para mantener buenos a los ciudadanos dentro de la red para que no causen accidentes.

1.20.4 Seguridad del BackOffice de Windows El Microsoft BackOffice es una suite de aplicaciones basadas en servidor que corren en sistemas Windows NT Server. Estas aplicaciones toman gran ventaja de los elementos de seguridad de Windows NT, incluyendo el directorio de servicios, acceso a cuentas de usuarios, listas de control de accesos (ACLs), auditoria y otras. A continuación se presenta las principales aplicaciones que conforman el BackOffice de Windows NT.

- *The Microsoft SQL Server.* Este es un componente de bases de datos relacionales para almacenar y administrar data.
- *The Microsoft SNA Server.* Este es un componente de conectividad de Host que provee acceso a clientes de Windows, Macintosh, DOS y OS/2 para AS/400 y mainframes de IBM.
- *The Microsoft System Management Server.* Este es un componente de administración de red que reduce el soporte y costos administrativos proveyendo una ubicación central para manejar el hardware y el software de la red, el software de distribución, resolución de problemas y manejo de aplicaciones.
- *The Microsoft Exchange Server.* Estos son componentes de correo electrónico y mensajería que provee una infraestructura de mensajes para mail y herramientas de colaboración. Microsoft Mail es el predecesor de esta herramienta.
- *The Microsoft Internet Information Server (IIS).* Este es el componente Web Server que viene incluido con Windows NT sin cargos adicionales.

De forma general podemos decir que estas aplicaciones funcionan como el HUB de una red de información, es decir, el punto de enlace y el puerto donde se unen las aplicaciones de más alto nivel. Algunas de las ventajas de este enfoque es el siguiente:

- Windows NT Server provee servicios de autenticación y transferencias seguras de data, y conoce la guía de referencia de niveles de seguridad C2.
- Los usuarios acceden una vez para obtener acceso a los recursos compartidos de SQL Server, el SNA Server, el Exchange Server y el System Management Server. Los administradores no necesitan bases de datos de cuentas por cada sistema.
- Los productos de BackOffice hacen uso del soporte de red que contiene Windows NT Server, incluyendo el soporte para redes populares como Ethernet, Token ring y Arcnet, así como protocolos populares como TCP/IP, IPX/SPX y NetBEUI.
- El soporte es provisto por diferentes plataformas de hardware, incluyendo máquinas y servidores basados en Intel, DEC Alpha, MIPS, y sistemas PowerPC. También se incluyen los sistemas multiprocesamiento.

1.20.5 Conexiones a Internet por medio del BackOffice En general, cualquier servidor Windows NT que esté ejecutando aplicaciones del BackOffice o que se conecte a otro servidor NT que si esté ejecutando dichas aplicaciones necesitará varios guardianes para prevenir los ataques de usuarios externos a los sistemas internos. Dicho esto, la solución a este problema es implementar un mecanismo que combina elementos de software y hardware para controlar el acceso y la salida de peticiones entre la red local e Internet. Nos referimos entonces a un Firewall. Los Firewalls (bien sea de router y/o de Proxy) funcionan como intermediarios entre el cliente de la red interna y la red externa (acceso a Internet). El Firewall recibe todos los requerimientos de los usuarios, los procesa y envía el resultado de la búsqueda en Internet al usuario que realizó la solicitud. Las ventajas de su implementación radican en que controla el acceso a la red interna y la salida a la red externa. Además el servidor NT puede funcionar como un proveedor de servicio de Internet de forma stand-alone.

1.21 Seguridad de SQL Server Microsoft SQL Server puede tomar ventaja de los elementos de seguridad de Windows NT Server, incluyendo cifrado de contraseñas, envejecimiento de contraseñas, restricciones de longitud mínima de contraseñas, y control de cuentas de usuarios. Cuando la seguridad integrada es colocada en un sitio, las cuentas de Windows NT son copiadas al SQL Server, de modo que, cualquier usuario que acceda a Windows NT también accederá a SQL Server. El acceso a SQL Server puede ser registrado en un archivo que indique la hora, la fecha y el intento exitoso o no exitoso de acceso al sistema que puede ser monitoreado por el administrador. El SQL Server provee un nivel de seguridad de mainframe para proteger la data sensible. Niveles de permisos a usuarios pueden ser implementados en tablas, vistas, procedimientos de almacenamiento y comandos SQL. Estos permisos también pueden ser aplicados sobre grupos, haciendo la administración de seguridad más fácil. La seguridad al nivel de campos también es soportada por SQL Server. Por último los flujos de datos generados durante transacciones distribuidas pueden ser encriptados para ofrecer altos niveles de seguridad para las transmisiones por cable.

1.21.1 Acceso a la data e Integridad SQL Server ofrece integridad de bases de datos. Todas las reglas de integridad, políticas de negocios y permisos de seguridad son manejadas e implementadas de forma centralizada. Esta centralización permite que cualquier cliente acceda a la base de datos sin las validaciones de integridad que han sido aplicadas sobre el servidor. Algunas políticas de integridad son:

- Niveles de seguridad sensitivos pueden ser implementados tanto para objetos como para comandos de la base de datos.
- Los usuarios pueden ser restringidos para acceder a distintos tipos de información, como números o fechas.
- Los administradores de bases de datos pueden otorgar permisos específicos a usuarios y a grupos tales como: select, insert, update, etc.

1.22.2 Protección de la Data Uno de los elementos más importantes, y hasta ahora no comentado, de SQL Server que asegura que la data siempre este disponible es que implementa un esquema de respaldo automático que puede generar copias en línea incluso cuando los usuarios están actualizando las bases de datos. Los administradores pueden usar el componente de programación periódica para realizar respaldos automáticos. El respaldo programado notifica a los administradores vía correo electrónico sobre el resultado o las fallas de las copias (backups).

1.23 Protección de Mensajes de Correos Para determinar algunas de las razones por las cuales se ha implantado este tipo de seguridad en el servidor de Exchange veremos algunos ataques que pueden realizarse al servidor de mensajería.

- Caballos de Troya y los virus pueden venir dentro de archivos adjuntos o attachments dentro de los mensajes. Usuarios insospechados pueden abrir y guardar dichos archivos y provocar fallos en el sistema, pérdidas de archivos o cualquier otro daño.
- Hackers que intentan interceptar paquetes y mensajes que están en tránsito, y leen o modifican dichos mensajes.
- Hackers pueden inundar las conexiones a Internet y sistemas de correos con mensajes que intentan producir ataques de negación de servicio.
- Los mensajes pueden ser falseados y aparezcan provenientes de fuentes desconocidas o de direcciones dentro de la organización.
- Los usuarios pueden transmitir información confidencial en sus mensajes, enviar información clave a usuarios desconocidos o no confiables, o simplemente inundan el sistema con mensajes en cadenas.

A este respecto, el servidor de Exchange ofrece múltiples opciones de seguridad, algunas de ellas son:

- *Encriptar los contenidos de mensajes y archivos adjuntos.* A través de esta opción el contenido de los mensajes y archivos adjuntos queda sellado de modo que solo pueda ser leído por el emisor y los receptores.
- *Firmas digitales.* Firma todos los mensajes de forma que los receptores puedan estar seguros de que el mensaje proviene de la fuente indicada. Autenticación.
- *Archivos de seguridad.* Muestra el nombre y la ubicación del archivo que contiene toda la información de seguridad del propietario.

- *Cambios de contraseña.*
- *Seguridad de Logoff.* Esta opción permite bloquear el sistema de mensajería de modo que nadie pueda enviar ningún mensaje desde una cuenta no autorizada, ni tampoco firmar los mensajes.
- *Configuraciones avanzadas de seguridad.*

Para implementar estas opciones de seguridad el Exchange Server se basa en los siguientes algoritmos:

- *RSA*. Algoritmo de cifrado y certificación de clave pública. Este protocolo provee las definiciones y el uso de los pares de claves públicas y privadas.
- *DES (Data Encryption Standard).* Este algoritmo permite codificar, cifrar y descifrar la data a través de una clave o número binario de 56 bits con 72 cuatrillones de combinaciones posibles.
- *CAST.* Los mensajes pueden ser cifrados en el MS Exchange Server y solo pueden ser descifrados por un receptor en MS Exchange Server que posea la correcta clave privada de encriptación. Las claves son intercambiadas utilizando algoritmos de clave pública de una longitud de 512 bits desde RSA Data Security, Inc. Las firmas digitales también son creadas a través de este mecanismo.

1.24 Acceso Remoto y Acceso a Internet Cada día son más los empleados o usuarios que necesitan y se conectan desde otros sitios distintos a su lugar de trabajo habitual, y requieren de mayor cantidad de dispositivos portátiles que les permitan acceder a la información desde cualquier punto, donde y cuando lo deseen. Esto es lo que se conoce como acceso de sitios remotos. En este sentido se pueden identificar dos métodos de acceso remoto:

- *Método de Control Remoto*. Con este método, un usuario que marque desde un sistema de control remoto (como es el caso de PCANYWHERE) conecta la máquina al sitio de marcado. Dicha máquina ejecuta todos los comandos por el usuario mientras que se logra la conexión. Solo el teclado y la pantalla actualizan la información que es enviada a través de la red.
- *Método de Acceso Remoto*. Con este método, un usuario que se conecta a través de un sistema de acceso remoto interactúa directamente con los sistemas en el servidor y/o en la red a la cual ha marcado. Los procesos toman lugar en la máquina del cliente. En la mayoría de los casos, los protocolos de red son usados a través de la línea.

Algunos tipos de ataques que pueden realizarse a través de este tipo de conexión son los siguientes:

- Hackers armados con '*war Dialers*' realizan cientos y cientos de llamadas por día buscando señales de marcado de módems. Una vez que las líneas de acceso remoto son localizadas, un Hacker puede centrarse en romper la seguridad del sitio. Una solución a este problema es responder las llamadas del módem luego de varias llamadas no al primer ring. Si no hay velocidad de respuesta el arma del Hacker inmediatamente buscará un nuevo número. Otra forma es cambiando el número telefónico a menudo.
- Un Hacker que obtenga un login y una contraseña válidas pueden acceder al sistema y robar información importante desde la comodidad de su hogar.
- Un Hacker que tenga acceso físico al sistema remoto que realiza las llamadas a la red local puede romper las secuencias de accesos y obtener la entrada. Llamadas de respuesta de seguridad pueden ser no efectivas, una vez que el usuario está en el sitio del cual se ha respondido.

Este tipo de problemas se resuelve limitando el acceso a través de elementos de hardware y software, definiendo políticas de seguridad y definiendo los privilegios de los usuarios que acceden de forma remota. Generalmente la opción inmediata y la solución más adoptada es la de crear un Firewall específico por cada tipo de conexión remota, teniendo siempre en mente que están basados en Windows NT.

1.25 Ataques en Windows NT Windows NT se ha convertido en uno de los sistemas operativos más populares que se usan en redes tanto publicas como privadas. Esto lo convierte en blanco para los ataques. La seguridad de Windows NT se vio incrementada debido a la publicación del articulo "Hobbit" en Avian Research sobre el Common Internet File System (CIFS) y el Server Message Block (SMB), las arquitecturas fundamentales de la arquitectura de la red NT. Desde entonces Microsoft ha resuelto la mayoría de los problemas que han aparecido, y ha mejorado notablemente su seguridad hasta el punto que es tan seguro como cualquier sistema UNIX, e incluso más, por los siguientes motivos:

- NT no dispone de la capacidad de ejecutar código de manera remota en el procesador del servidor: Cualquier programa que se lance se ejecuta en el procesador del cliente y en su memoria principal.

- El derecho a iniciar la sesión de forma interactiva en la consola esta restringido por defecto, a unas cuantas cuentas administrativas (solo para NT Server), por lo que, a menos que un atacante viole esas cuentas, no conseguirá casi nada (existe algunas formas de evadir esto, pero muy difícil).
- El acceso al código fuente de NT ha sido bastante restringido por parte de Microsoft, por lo que el fatal desbordamiento de memoria que agobia al mundo UNIX no suele ocurrir tan a menudo.

Pero a pesar de esto Windows NT es más inseguro de lo que podría ser, esto es debido: La compatibilidad con versiones anteriores y la facilidad de uso. Una muestra de esto es el uso de los protocolos NetBIOS/CIFS/SMB y un viejo algoritmo LanManager para encriptar las contraseñas de los usuarios. En cuanto a la simplicidad de su interfaz lo hace atractivo para administradores novatos que no tienen muchos conocimientos de seguridad que solo necesitan seguir un asistente para instalar y configurar el sistema.Para dar a conocer las principales debilidades de Windows NT se seguirán los pasos clásicos del repertorio de un atacante: conseguir los privilegios de acceso como súper usuario, consolidad su posición y borrar sus huellas. En la siguiente tabla se da una visión de los temas cubiertos.

Cómo ser Administrador
Adivinar Contraseñas: Manual Automática Escuchar y pasar la información sin descifrar
Ataques Remotos: Desbordamiento del Búfer de Memoria Negación del Servicio
Escalada de Privilegios: Hoovering GetAdmin Sechole Troyanos y Claves de Registro
Consolidación de Privilegios
Hacer Craking el SAM: Obtener el SAM L0phtcrack Otros crakers NT
Abuso de Confianza: ISA Secrets Claves de registro de conexión Automática Registro de pulsaciones del teclado
Control Remoto y Puertas Traseras: Remote.exe Escuchas netcat NetBus Back Orifice2000 WinVnc
Borrar Huellas
Desactivar la Auditoria.
Limpia los Registros de sucesos
Archivos Ocultos: attrib Streaming

1.26 Búsqueda del Administrador: La primera regla importante es que si el intruso en un sistema remoto no es administrador no tiene nada que hacer. NT no tiene la capacidad de ejecutar comandos de forma remota y si lo tuviera el inicio de la sesión interactiva esta restringida a los Administradores. Es por esto que los atacantes buscan cuentas del tipo Administrador y para eso se valen de los siguientes métodos:

- Adivinar las contraseñas de la red. Las tres principales técnicas que existen para adivinar las contraseñas en NT en la red son: Manual, Automática y escuchando los inicios de sesión para obtenerla directamente.
    - Adivinar las contraseñas manualmente. Esta técnica se basa en las debilidades de los usuarios:
        - Los usuarios tienden a escoger la contraseña más fácil de recordar, es decir, **ninguna**.
        - Los usuarios escogerán algo que sea fácil de recordar, como su nombre, apellido, o muy obvio como el nombre de la organización.
        - Existe gran cantidad de software que se ejecuta bajo el contexto de una cuenta de usuario NT, generalmente con el paso del tiempo estas cuentas llegan a ser de conocimiento público; estas cuentas suelen tener muchos privilegios que pueden ser aprovechados por los intrusos.
        - También se pueden adivinar las contraseñas a través de la línea de comandos, mediante el comando net use. Si se especifica un * en vez de la contraseña, el sistema remoto pedirá una.

          C:\net use 192.168.202.44\IPCS * /user:Administrator
          Type the password for \\192.168.202.44\IPCS:
          The command completed successfully

Los atacantes, normalmente intentarán adivinar las contraseñas de cuentas locales, en lugar de las cuentas globales de los controladores de dominio NT. Las cuentas locales son más débiles por la poca seguridad implementada por los usuarios, mientras que las cuentas de los sistemas centrales de la empresa suelen cumplir mejor con las políticas y normas de la organización. Además NT Workstation permite que cualquier usuario inicie una sesión de forma interactiva, esto hace más fácil la ejecución de comandos en forma remota.

- Detección automática de las contraseñas: Existen en el mercado algunos programas que permiten encontrar las contraseñas de forma automática, dos de estos programas son Legión y NetBIOS Auditing Tool (NAT). Estos programas explorar distintos rangos de direcciones IP de clase C para encontrar usuarios y contraseñas.
- Escuchar y pasar la información sin descifrar en el intercambio de contraseñas en la red. Es poco probable que un atacante sea capaz de escuchar el intercambio de contraseñas en el inicio de sesión de Windows NT, pero existen herramientas que hacen el trabajo por el, una de las más populares es L0phtcracl de un grupo de Hackers autodenominado L0pht, la cual trabaja generalmente fuera de línea contra la base de datos de contraseñas de NT que ha capturado, por lo que el bloqueo de dicha cuenta no es su objetivo y puede continuar el proceso de manera infinita. Obtener el archivo de contraseñas no es una tarea trivial, pero es factible. Las ultimas versiones de este software incluyen una función llamada *SMB Packet Capture* que evita la necesidad de capturar el archivo de contraseñas. Esta función escucha el segmento de red local y escucha los inicios de sesión individual entre sistemas NT, captura la contraseña, descifra la información de la contraseña y realiza el proceso de ingeniería inversa a la encriptación de la contraseña (proceso conocido como **craking**). Esta herramienta es tan poderosa que alguien que pueda conectarse a la red durante largos periodos de tiempo, puede obtener el estatus del administrador en pocos días.
- El hecho de que la red tenga una arquitectura conmutada no quiere decir que este fuera de peligro ni que se puedan capturar las contraseñas. Cualquier atacante podría utilizar parte de la ingeniería social que puede encontrar en la red, como por ejemplo. "Enviar un correo electrónico al individuo o a una compañía entera, incluyendo en el la siguiente línea: ////<nombre del pc>/nombrecompartido/mensaje.html Cuando las personas pulsen sobre este url, estará enviando sus contraseñas para la autentificación".

1.27 Como defenderse de la captura de las contraseñas Existen varias técnicas que pueden impedir o al menos, o al menos hacer más difícil que sean capturar las contraseñas:

- Si el sistema Nt es un host en internet no debe acceder a las solicitudes para compartir recursos en Windows: bloquear a los puertos TCP y UDP 135 –139 en el Firewall frontera o el router y

desactivar los enlaces a WINS Client(TCP/IP) para cualquier adaptador conectado a redes publicas. Con esto se desactiva cualquier puerto NetBIOS

- Para servidores de archivos NT debe mantener la conectividad de Windows, esta medida no será suficiente, entonces se hace necesario medidas tradicionales como el bloqueo de cuentas después de un determinado numero de intentos de inicio de sesión fallidos, forzar el empleo de políticas de contraseñas eficaces y llevar un registro de los intentos fallidos.

1.28 Políticas de cuentas Una recomendación es utilizar la herramienta de administración de cuentas del administrador de usuarios, con esta función se puede aplicar ciertas restricciones en las contraseñas de las cuentas, como longitud mínima y la unicidad de la contraseña en el tiempo. También es posible bloquear una cuenta después de un número determinado de intentos de inicio de sesión fallidos. Además esta herramienta permite a los administradores la desconexión de un usuario cuando expire el tiempo de conexión.

1.28.1 Passfilt Se puede mejorar la seguridad con un dll llamado Passfilt que se incluye desde el Service Pack 2, este dll asegura una elección de contraseña fuerte, evitando que alguien omita las reglas por error o por pereza. Cuando esta instalado, requiere que las contraseñas, tengan al menos, seis caracteres de longitud, no debe contener el nombre de un usuario o cualquier parte de un nombre completo y deben contener al menos tres de los siguientes caracteres:

- Letras mayúsculas del Ingles (A...Z)
- Letras minúsculas del Ingles (a...z)
- Números arábigos occidentales (0...9)
- Meta caracteres no alfanuméricos (@, #, %, etc)

1.28.2 Passprop Otra herramienta incluida en el kit de recursos de NT, esta define los requisitos para las cuentas de dominios de Windows NT:

- Si es activado las contraseñas deben tener una mezcla de letras mayúsculas y minúsculas, así como, caracteres alfanuméricos.
- Controla eel bloqueo de cuentas del administrador. Desafortunadamente la cuenta original (RID 500) no se puede bloquear en NT, lo que le brinda a los posibles atacantes infinidad e ilimitada cantidad de oportunidades para obtener la contraseña. Passprop elimina la restricción por defecto de NT para bloquear esta cuenta.

Como evitar que se escuche y que se pase la información sin descifrar en el intercambio de contraseñas en la red. Una de las mejores recomendaciones para evitar este tipo de ataque es migrar la red hacia arquitecturas de red conmutadas, pero aun así no se libera del eventual ataque. Dos de la medidas que se pueden tomar para evitarlo son:

- Desactivar la autentificación LANMAN a favor de "Pasar el HASH": El Service pack de Windows NT 4.0 ha añadido una clave de registro y un valor que impedirán que el host NT acepte la autentificación LANMan. Lamentablemente esta medida no se puede implantar si tiene estaciones de trabajo del tipo win9x y Windows para grupos de trabajo ya que negara los servios a los mismos.
- Activar la firma SMB: Esta herramienta viene en el Service Pack 3 o superior. La firma SMB requiere que todo paquete SMB que se envié dentro de clientes NT correctamente configurados y servidores, se debe verificar criptográficamente. Al activarlo se observa entre un 10 y 15 por ciento de disminución en el rendimiento de la red, además no soporta clientes win9x

1.29 Auditorias y Registros Es recomendable que se lleve un registro de conexión fallida utilizando las facilidades que brinda el administrador de usuarios. Los reportes generados pueden ser revisados por el administrador o por herramientas que buscar y notifican inmediatamente eventos que puedan indicar posibles ataques.

1.30 Ataques remotos: Negación de servicios y desbordamiento del búfer de memoria Otra manera de atacar a Windows NT es localizar algunos de los defectos inherentes a la arquitectura del mismo que se podría aprovechar de forma remota para poder entrar al sistema.

1.30.1 Desbordamiento del búfer de memoria La amenaza más peligrosa lo constituye los denominados búfer overflows o desbordamiento del búfer, estos se producen cuando un programa no comprueba si la entrada de datos tiene la longitud adecuada, por lo que cualquier entrada no esperada "desbordada" la pila de ejecución del CPU. Si un programador oportunista elige esta entrada, la pude utilizar para ejecutar el código que se le antoje. Normalmente suele ser un ejecutable que le de privilegios del sistema. Para evitar el desbordamiento del búfer de memoria, se debe ser extremadamente cuidadoso al ejecutar programas de fuentes poco fiables, y se debe, verificar la autenticidad de todos los archivos utilizados, especialmente archivos del sistema utilizados en el proceso de inicio. Además, existen herramientas que buscan entradas no esperadas en los programas y archivos.

1.30.2 Negación de Servicio (DoS) La idea de este ataque en general es que. Frecuentemente, resulta mucho más fácil desorganizar el funcionamiento de una red o sistema que acceder realmente al mismo. Los protocolos de red como TCP/IP para el empleo de una comunidad abierta y confiada. Un ataque Dos consta esencialmente de la negación de un servicio o de la desorganización a los usuarios legítimos, redes, sistemas u otros servicios. La intención de cualquier ataque de este tipo, es dañina por naturaleza y generalmente requiere poca inteligencia, pues la mayoría de los recursos para cometer un ataque de este tipo se consiguen en la red. Existen muchos tipos de ataques DoS, muchos de ellos pasan inadvertidos hasta el momento en que colapsan el servicio Una medida puede ser desactivar la función de difusión de los Routers frontera y monitorear constantemente el trafico para detectar posibles ataques de este tipo y así poder tomar las medidas necesarios para controlar esta situación.

1.30.3Escalada de Privilegios Existen ciertas herramientas que permiten obtener privilegios adicionales de una cuenta de usuario, pero para ello necesita ejecutar desde la cuenta del usuario NT típica, ya que por los privilegios que posee no puede realizar inicios de sesión interactivos, si el administrador del sistema ha cometido errores críticos es posible utilizar estas herramientas para obtener muchos privilegios. A continuación alguna de las técnicas fundamentales para conseguir los privilegios de administrador:

- *Aspirar información* Cuando un atacante se apodera de una cuenta limitada, comienza a buscar por todos los medios recopilar información necesaria que le permita acceder a los servidores y aumentar sus privilegios. Para evitar la aspiración de información. Una de las recomendaciones mas útiles que hacen los expertos consiste en conectarse como un usuario conocido y probar todo lo que pueda hacer empleando esta técnica, después, se debe filtrar y reforzar todas las áreas donde haya encontrado debilidades
- *GetAdmin* es un pequeño programa escrito por Komstamtin Sobolev que añade a un usuario al grupo de Administradores local. Utiliza una rutina del núcleo de NT de bajo nivel para configurar una bandera global que permite el acceso a cualquier proceso que se este ejecutando, y, a continuación usa técnica denominada DLL (infección para insertar un código maligno en un proceso que tenga el privilegio de añadir usuarios al grupo de administradores (este proceso se llama winlogon). El agujero producido por getadmin puede ser arreglado mediante una utilidad de Microsoft llamada pos-SP hotfix.
- *Sechole* funciona de manera similar a getAdmin añade al usuario actual grupo de administradores local, una versión mas reciente introduce al usuario como miembro de administradores de dominio. Microsoft tiene una utilidad para la técnica del sechole y la ejecución web remota denominada priv-fix. Una medida es auditar los privilegios de ejecución en el sistema de archivos del servidor web, y configurarlos de manera individual dependiendo del la necesidades de cada uno.
- *Troyanos y claves de registro ejecutables.*Un troyano es un programa que aparenta realizar una función util pero, en realidad, ejecuta algo completamente diferente de forma oculta. Existen muchas maneras de renombrar utilidades básicas de NT. Un troyano que ataque a NT puede sustituir regedit.exe por un archivo por lotes denominado regeidt.cmd. Cuando el administrador llame a "regedit" ejecuta alguna tarea, se ejecuta el archivo por lotes que por lo general contiene una instrucción de agregar a un usuario. La mejor manera de evitar estos ataques es monitorear para encontrar comportamientos sospechosos como por ejemplo, que el shell de comandos aparezca brevemente antes de que aparezca una falla en alguna aplicación.

1.30.4 Consolidar la posición Una vez que un ente logra introducirse en el grupo de usuarios, buscara la manera de aumentar sus privilegios. A continuación se presentan algunas técnicas y herramientas que utilizan para intentar conseguir su objetivo.

- *Cracking del SAM* Después de que un atacante ha los privilegios de administrador, tiene el camino libre hacia el Security Accounts Manager (SAM) o Administrador de Cuentas de Seguridad en NT. El SAM contiene los nombres de usuario y las contraseñas encriptadas de todos los usuarios del sistema local, o del dominio de maquina en un controlador de dominio. Pero a pesar de que las contraseñas se encuentran encriptadas esto no garantiza el mantener a los atacantes alejados, pues Microsoft para mantener la compatibilidad con sistemas anteriores hizo una concesión de clave con NT que disminuyo la seguridad del SAM. SAM utiliza un algoritmo de hashing para poder ser compatible con LanManager de NT. Este débil algoritmo ha sido descifrado, por lo que se ha convertido en el talón de Aquiles que permite, en la mayoría de los casos, descubrir trivialmente una contraseña. Por ejemplo la versión 2.5 de L0phtcrak puede romper una clave alfanumérica en menos de 24 hora utilizando un procesador Pentium II a 450 Mhz. El primer paso para obtener las claves o contraseñas es obtener el SAM. NT guarda este archivo con el nombre de SAM. Este archivo se encuentra en el directorio %systemroot%\system32\config, que esta bloqueado siempre que se esta ejecutando el sistema operativo. Para obtener el SAM existen cuatro formas:
    - *Arrancar el equipo con un sistema operativo distinto:* Tan solo con arrancar el equipo con un disquete con el sistema operativo DOS. Si el equipo ejecuta particiones con el formato NTFS, entonces será necesario incluir también el controlador de archivos del sistema NTFS, lo que permitirá montar la unidad como unidad lógica dos.
    - *Obtener una copia de seguridad del SAM del directorio de reparación:* Cuando se ejecuta la utilidad de reparación del disco (rdisk) con la opcion /s para hacer una copia de seguridad de la información clave de la seguridad del sistema, se creara una copia comprimida del SAM, denominada sam._, en el directorio %systemroot\repair%
    - *Extraer la información del SAM:* existe una utilidad llamada pwdump que permite guardar la información en un archivo texto para su posterior uso.
- *Escuchar el intercambio de contraseñas en NT:* Una de las características más poderosa de L0phtcrack es su capacidad de extraer hashes de contraseñas, solo se debe configurar y correr esta utilidad para obtener los resultados esperados. Existe otra herramienta basada en diccionarios que permite hacer cracking de los archivos de contraseñas, además permite hacer cracking con varios algoritmos de encriptación. Esta herramienta se le llama "John el Destripador".

Para evitar consolidar la posición es conveniente aplicar las siguientes medidas:

- Elegir contraseñas fuertes para NT. Esta o es la mejor defensa ante este tipo de ataque, pero, si lo hace mas difícil, es decir el tener una fuerte política para el uso de las contraseñas evita en gran medida que estas sean descubiertas de manera trivial.
- Proteger el SAM es critico impedir el acceso al SAM, la única forma es restringir el acceso a los servidores para que ninguna persona entre a ellos con un disquete y arranque en modo DOS para obtener una copia de el, o que, duplique la copia de seguridad sam._ del directorio repair.
- Implementación de SYSKEY. Esta utilidad se introdujo desde la publicación del Service Pack 2 y mejora la encriptación del SAM. SYSKEY establece una clave de encriptación de contraseñas criptográficas con 128 bits, contrariamente a los mecanismos de 40 bits que se establecen de forma predeterminada.

1.30.5 Abuso de Confianza capturar la cuenta del Administrador de un sistema NT no implica necesariamente que se capture todo el dominio, lo mas probable es que sean servidores de aplicaciones individuales, no controladores de dominio. Sin embargo, existen opciones para acceder a todo el dominio.

- Copia especular de las credenciales del administrador de dominio y local. Es un agujero peligroso del cual se le puede sacar partido, en realidad es una mala administración de la cuenta: guardar las credenciales de los usuarios de dominio en servidores NT autónomos o estaciones de trabajo individuales. En un mundo perfecto, nadie iniciaría una sesión en un sistema NT individual como Administrador local utilizando el mismo nombre de usuario y contraseña que en su cuenta de dominio, ni la crearía con estas características. Pero, lamentablemente no estamos en un mundo perfecto. Este pequeño desliz de seguridad es el responsable de muchos de los casos de violación de dominios NT. Hay tres puntos que se deben vigilar:

- Las cuentas de administrador local que utilicen las mismas contraseñas que las del grupo de administrador de dominio.
- las cuentas locales que tengan nombres de usuarios y contraseñas idénticas a las cuentas de dominio, especialmente los miembros de los administradores de dominio.
- La información contenida en los campos de comentario que den pistas sobre las credenciales de la cuenta de dominio.

La mejor medida para evitar este tipo de ataques es definir complejas contraseñas para el administrador de dominio y cambiarlas regularmente (cada 30 días o menos). Además no se deben usar las cuentas del usuario para funciones administrativas, ya que esto dificulta la auditoria de las mismas, es recomendable crear una cuenta para estos fines.

1.30.6 LSA Secrets En 1997 Paúl Ashton envió el código fuente de esta utilidad que permite ver el contenido de la información de seguridad almacenado por el Local Security Authority (LSA), incluyendo contraseñas (texto puro), hashes de contraseñas almacenadas en cache de los últimos usuarios que se conectaron a la maquina, contraseñas de texto puro FTP y WEB, nombre y contraseñas de accesos telefónicos RAS, contraseñas de maquinas para acceder al dominio entre otros.

1.30.7 Conexión automática de las claves de registro Se puede configurar NT para que permita la conexión automática cuando arranque la maquina utilizando la clave KLM\SOFTWARE\Microsoft\Windows NT\Current Versión\Winlogon\AutoAdminLogon. Aunque esta utilidad es muy buena para permitir a usuarios autorizados se conecten a un servidor sin necesidad de pedirles sus credenciales, guarda en el sistema local credenciales con gran poder, en forma de texto en el sistema de registro KLM\SOFTWARE\Microsoft\Windows NT\Current Versión\Winlogon\AutoAdminLogon\DefaultDomainName, DefalyUserName, DefaultPassword Para desactivar la conexión automática, se debe borra el valor DefaultPassword almacenado en esta clave, Además, también se debe borrar la clave AutoAdminLogon, o cambiar su valor a 0.

1.30.8 Registro de pulsaciones del teclado Estas son aplicaciones que se colocan entre el hardware del teclado y el sistema operativo, para así poder registrar en un archivo local oculto cada una de las pulsaciones del teclado hechas por el usuario Es dificil detectar la presencia de un programa de registro de pulsaciones de teclado debido a su bajo nivel de filtración en el sistema, sin embargo, realizando auditorias permanentes a los sistemas se puede descubrir muchos de estos programas.

1.30.9 Control remoto y puertas traseras Se ha dicho que NT no permite la ejecución de comandos remotos, pero si se obtiene acceso como Administrador, se abre una infinidad de posibilidades. Línea de comandos remotos de NTRK: remote.exe. NTRK dispone de dos utilidades que permiten ejecutar comandos de forma remota: el Rmote Command Line (remote.exe, línea de comandos remota) y el Remote Command Service (rcmd.exe y rcmdsvc.exe, cliente y servidor respectivamente). Instalar y configurar esta utilidad es especialmente difícil y aun mas difícil es que funciones para los propósitos que se desean. Shells remotos mediante programas de escucha netcat. Otra manera de configurar una puerta trasera es utilizando TCP/IP, mediante la utilidad llamada netcat. Se puede configurar netcat para escuchar cierto puerto y lanzar un ejecutable cuando un sistema remoto se conecte a ese puerto. Es posible configurar este programa para poner en marcha un shell de NT, y así, darle a los usuarios remotos la posibilidad de ejecutar comandos.

1.30.9 NetBuss es la mayor utilidad de administración remota y espionaje Back Orifice BO. Una vez instalado y configurado (se puede instalar mediante un troyano) en la maquina que se quiere atacar, la consola de NetBus esta en la capacidad de controlar el sistema remoto en todos sus sentidos.

1.30.10 Back Orifice 2000 Es una utilidad que permite funciones de control de acceso remoto que le da control al atacante del sistema capturado. Es una herramienta que utiliza la GUI de Windows y una conexión que administre un sistema remoto.

1.30.11 Medidas para Control remoto y puertas traseras teniendo en cuenta que para instalar y obtener los privilegios que le permitan tomar al sistema por esta vía es teniendo una cuenta de Administrador y que acceden a casi todos los recursos de la arquitectura de NT, además de que pueden modificar casi todos los

nombres de los archivos necesarios y configurarles de un numero ilimitado de formas, la tarea es difícil, sin embargo se pueden tomar las siguientes medidas:

- *Nombres de archivos* esta medida solo resulta efectiva para atrapar intrusos poco creativos, pues la mayoría se toma la molestia de renombrar y ocultar los archivos necesarios del programa
- *Entradas de registro e*ste método intenta buscar valores de registro, ya que la mayoría de las aplicaciones intentan encontrar determinados valores en aplicaciones especificas.
- *Ocultar el rastro* una vez que los intrusos han accedido al sistema con privilegios de administrador, su principal empeño consiste es evitar ser detectados. Entonces después de haber accedido al sistema destino, instalaran puertas traseras y ocultaran un grupo de actividades para su uso posterior con el fin de asegurarse su acceso en un futuro de manera fácil. Los principales ataques en este sentido son:
    - Desactivar la auditoria seguramente el administrador del sistema tiene algo de experiencia en seguridad, tendrá activado los procesos de auditoria, tal y como se recomienda en secciones anteriores. así que, lo primero que hará el intruso es verificar las políticas de auditoria definidas en el sistema para cambiarlas de manera que no sea posible tener algún rastro.
    - Borrar el registro de sucesos una vez autentificado el host remoto el atacante podrá abrir leer y limpiar los registros de sucesos.
    - Ocultar los archivos guardar un grupo de utilidades en el equipo para utilizarlas posteriormente supone un gran ahorro de tiempo para el atacante. Pero, por otra parte, se pueden convertir en tarjetas de visita que pongan sobre aviso de la presencia de intrusos a cualquier administrador del sistema.
- Attrib no existe nada mas sencillo que ejecutar el comando attrib de DOS. Este proceso permite ocultar archivos y directorios.
- Streaming de archivos NTFS si el sistema de archivos esta ejecutando el sistema de archivos de Windows NTFS los intrusos tienen una técnica alternativa para ocultar archivos. NTFS permite el empleo de múltiples streams de información dentro de un archivo.

2.0 UNIX Y Linux

2.1 INTRODUCCIÓN Unix fue creado a principios de los sesenta con la idea de hacer un sistema operativo que facilitase la labor a los programadores. A la conclusión que se llegó es que la mejor forma es establecer un conjunto definido de pequeñas herramientas que hagan una determinada labor muy bien. A partir de la unión de esas herramientas se pueden realizar labores más complejas mediante la comunicación de los resultados de unas se conviertan en entradas de otra. LINUX es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado. La primera es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo. La segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (Kernel) más un gran número de programas / librerías que hacen posible su utilización Las funciones principales de este sistema operativo son:

- *Sistema multitarea:* Es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.
- *Sistema multiusuario:* Varios usuarios pueden acceder a las aplicaciones y recursos del sistema al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar varios programas a la vez (multitarea).
- *Shells programables:* Un shell conecta las ordenes de un usuario con el Kernel (el núcleo del sistema), y al ser programables se puede modificar para adaptarlo a tus necesidades. Por ejemplo, es muy útil para realizar procesos en segundo plano.
- *Independencia de dispositivos:* Admite cualquier tipo de dispositivo (módems, impresoras) gracias a que cada vez que es instalado uno nuevo, se añade al Kernel el enlace o controlador necesario con el dispositivo, haciendo que el Kernel y el enlace se fusionen. Posee una gran adaptabilidad y no se encuentra limitado como otros sistemas operativos.
- *Comunicaciones:* Es el sistema más flexible para poder conectarse a cualquier computador del mundo. Internet se creó y desarrollo dentro del mundo de Unix

La seguridad UNIX tiene una reputación de complejidad y dificultad de uso. La buena noticia es que no es difícil, la mala noticia es que es compleja. El verdadero problema para la mayoría de las organizaciones es qué cantidad y qué tipo de seguridad satisface los requerimientos de su ambiente particular. Encontrar la respuesta a estas preguntas está lejos de ser un asunto trivial. Comienza por decidir qué necesitas asegurar y cuánto puedes gastar para protegerlo, finaliza con la creación de una política de seguridad que guíe las especificaciones, implementación, gestión y reportes de aspectos técnicos. Estos aspectos incluyen detalles técnicos, organizacionales y de personal. La seguridad de los sistemas basados en UNIX es fundamentalmente la misma que la seguridad de cualquier otro sistema o componente de red. Los sistemas UNIX frecuentemente se encuentran dentro de una infraestructura. En las pocas excepciones, como los sistemas de uso sencillo para el control en tiempo real y aplicaciones militares específicas, el enfoque de la seguridad normalmente puede ser resumido a factores físicos y de personal. Sin embargo, los sistemas UNIX usualmente son sólo una parte de una infraestructura de computación mayor, que incluye otros sistemas operativos y componentes de red. Aunque en un principio y según uno de sus creadores, Unix no se diseñó para ser seguro, a finales de los 80 se convirtió en el primer sistema operativo en alcanzar niveles de seguridad casi militares"C2". En la actualidad se puede considerar el sistema operativo de propósito general más fiable del mercado. El problema es que en muchas ocasiones se pone a trabajar a Unix tal y como se instala por defecto, lo que convierte a cualquier sistema operativo, Unix o no, en un auténtico agujero en cuanto a seguridad se refiere.

2.2 Standard de seguridad X/Open ofrece a los vendedores de sistemas basados en UNIX un conjunto de pruebas. Si el vendedor pasa la prueba, X/Open lo marca como capacitado con sus especificaciones comunes de UNIX. Esta marca permite al vendedor utilizar "UNIX" en el nombre de sus derivados UNIX. Esto también asegura al vendedor que su producto está al nivel de los otros vendedores marcados. Como X/Open es el que mantiene actualmente la marca UNIX, este es un gran paso en la evolución de UNIX. El surgimiento de los sistemas distribuidos y cliente/servidor como requerimientos comerciales está solicitando a los vendedores implementar nuevos modelos de seguridad en sus productos UNIX. Los

vendedores de sistemas UNIX están adoptando agresivamente los estándares relativamente nuevos en esta área. Los sistemas UNIX que tienen elementos de seguridad alineados con las especificaciones de seguridad existentes están en surgimiento. Estos estándares incluyen el POSIX de IEEE's, el Ambiente de Cómputo Distribuido (DCE) de OSF y System V release. Con respecto a los estándares de interfaz de seguridad, la comunidad de seguridad general de interfaz para programadores de servicios y aplicaciones de internet (GSSAPI) está prevaleciendo como la interfaz de servicios de seguridad de preferencia.

2.3 Los Servicios ¿Qué es lo primero a solucionar? los servicios. Linux está diseñado desde el punto de vista de un servidor de red. Esto significa que ofrece servicios a la red y uno de los problemas que podemos tener son estos. Los servicios son puertas con las cuales los usuarios u otros servicios pueden interactuar. Cuantas más puertas tengamos en una casa menos segura es ésta. Estos servicios se dan en unos puertos determinados. A cada puerto se le nombra por un número pudiendo ir desde 1 hasta 65536. Veamos cuáles son esos servicios que Linux trae (algunos abiertos por defecto), a qué puertos se asocian, qué hacen y con cuáles nos debemos quedar.

Servicio / Puerto / Protocolo	Descripción	¿Mantenerlo?	Localización
echo / 7 / tcp-udp	Todo lo que se mande a ese puerto lo devuelve.	No	inetd.conf
daytime / 13 / tcp-udp	Devuelve la fecha y la hora del sistema.	No	inetd.conf
ftp / 21 / tcp	Servidor FTP.	Quizás/restringir	inetd.conf
telnet / 23 / tcp	Permite conectarnos y abrir una consola remotamente.	Sí/restringir	inetd.conf
smtp / 25 /tcp	Gestiona la distribución del correo de la máquina.	No	/etc/rc.d
timeserver / 37 / tcp-udp	Devuelve la hora el sistema	No	inetd.conf
named / 53 / tcp-udp	Servidor de nombres (DNS)	No	/etc/rc.d
gopher / 70 / tcp	Sistema de indexación de los servidores FTP (obsoleto)	No	inetd.conf
finger / 79 / tcp	Devuelve información sobre los usuarios del sistema	No	inetd.conf
http (www) / 80 / tcp	Servidor WWW	No	/etc/rc.d
linuxconf / 98 / tcp	Sistema de configuración remota	No	inetd.conf
pop2 / 109 / tcp	Servidor de correo Pop versión 2	No	inetd.conf
pop3 / 110 / tcp	Servidor de correo Pop versión 3	No	inetd.conf
rpcbind /111 / tcp-udp	Servicio de RPC (portmapper)	No	/etc/rc.d
auth (ident) / 113 / tcp	Identifica y registra a los usuarios que hace uso de servicios tcp	Sí	inetd.conf
innd / 119 / tcp	Servidor de News	No	/etc/rc.d

netbios / 137-138-139 / tcp-udp	Servidor Samba. Windows for Workgroups	No	/etc/rc.d
imap2 / 143 / tcp	Servidor de correo Imap versión 2	No	inetd.conf
login / 513 / tcp	Permite logins remotos (rlogin) a usuarios autorizados	No	inetd.conf
shell / 514 / tcp	Permite shells remotos (rshell) a usuarios autorizados	No	inetd.conf
syslog / 514 / udp	Registra todos los sucesos del sistema y los guarda en logs	Sí	/etc/rc.d
lpd / 515 / tcp	Servidor de Impresión	Sí	/etc/rc.d
uucp / 540 / tcp	Antiguo protocolo de comunicación de unix	No	inetd.conf
mountd / 635 / udp	NFS mount daemon	No	/etc/rc.d
nfsd / 2049 / udp	Sistema de archivos de red de Unix	No	/etc/rc.d
x-windows / 6000	Acepta conexiones de servidores X autorizados	Si/restringir	host -

¿Qué significa 'Quizás'? se refiere a que sólo deberemos dejarlos abiertos si los vamos a usar. Si no necesitamos un servidor FTP, deberíamos desactivar estos servicios. En el caso del servidor SAMBA y NFS, sólo nos interesa tenerlo si queremos compartir información con otras máquinas Windows (samba) o Unix (nfs), si no es así no lo usaremos y lo mejor será cerrarlo, ya que tienen un largo historial de problemas de seguridad y requieren una configuración cuidadosa. Si no hay más remedio que usarlos, hay que configurarlos bien y estar atentos a posibles parches.

2.4 Seguridad de las cuentas uno de los aspectos más importantes en cuanto a la seguridad de las cuentas son los passwords o claves de acceso. A continuación se presenta una lista de alternativas que NO deben ser incluidas en los passwords:

- El login de ninguna forma: inverso, truncado, etc.
- Nombres de esposa, hijos, ni otros nombres comunes.
- El nombre propio o apellido seguidos o precedidos por un dígito.
- Número de cédula, teléfono, seguro social, marca de auto, etc.
- Nombre de la calle donde vive, urbanización, etc.
- Todos los dígitos o la misma letra.
- Palabras de diccionario.

A continuación se presenta una lista de alternativas que se deben utilizar para los passwords:

- Más de 5 caracteres. En Unix por lo general acepta hasta 8.
- Letras mezcladas con dígitos y signos de puntuación.
- Fácil de recordar, para no anotarlo en papel.
- Que se escriba rápidamente.
- Tomar las letras de una frase fácil de recordar, pensamiento, poema, etc.

Adicionalmente se deben seguir una serie de medidas para mantener la seguridad de las cuentas. A continuación se mencionan algunas:

- Lo primero será no dejar los password accesibles a los usuarios del sistema. Los passwords están encriptados, pero un cracker puede usar programas para saltarse esta encriptación y con la

capacidad de los PCs actuales es cuestión de tiempo el que consiga todos los passwords por fuerza bruta, es decir, probando todas las posibilidades. Para esto se guardarán en un archivo que se llamará /etc/shadow. Este archivo contendrá las passwords encriptadas e información sobre su caducidad, tiempo para cambiarse, etc. Y lo más importante: sólo tendrá privilegios de lectura para Root, evitando que cualquier intruso se las lleve. Para aplicar esto, se debe ejecutar como Root el comando: pwconv. Habrá creado un archivo /etc/shadow (si no existía) y habrá metido todos los passwords, junto con otra información. Si ya existía, lo actualiza. Tras hacer esto, lo mejor para comprobarlo es activarse desde la consola y ver si funciona correctamente. Si hay algún problema y requiere volver a poner todas los passwords en el /etc/passwd, se debe colocar: pwunconv

- No se debe olvidar eliminar las cuentas que ya no se vayan a usar más.
- La cuenta Root es la más peligrosa. Se debe usar sólo cuando sea necesario. Para el trabajo diario es más conveniente crear una cuenta con el comando useradd.
- Se debe revisar el path de la cuenta Root en los archivos de inicialización (.login, .cshrc, .profile, etc.). El comando path o la variable de entorno PATH definen los directorios de búsqueda de los ejecutables. El directorio ".", es decir, el actual, NUNCA debe aparecer en el path del Root.
- El archivo /etc/securetty establece la lista de los terminales desde los cuales el Root puede hacer login. En algunas distribuciones, por defecto, queda limitado a la consola. Si es así, NO DESHABILITARLO. Se debe comprobar de todas formas que en este archivo sólo aparezca tty1...tty8.

2.5 Seguridad de los archivos Como se mencionó anteriormente, Linux es un sistema multiusuario. La máquina que posee el sistema que sirve a los demás usuarios se llama Host. Una posibilidad de entrada de diferentes usuarios al mismo sistema es por medio de las consolas virtuales. La tecla ALT combinada con las teclas que van desde F1 hasta el F6 abren una nueva consola en la que puede hacer logon un nuevo usuario. Hay diferentes tipos de usuario, entre los que distinguimos los dos tipos más importantes: Los administradores y los usuarios comunes. El usuario administrador (Root) tiene un completo control sobre el sistema. Puede guardar, configurar, borrar, o hacer lo que quiera con lo que hay dentro del sistema. Un usuario común, en cambio, sólo puede manejarse con limitados recursos dentro del mismo sistema. Esto es porque hay información y cosas que dichos usuarios no deben tener a su alcance por medidas de seguridad. Adicionalmente, los usuarios pueden ser agrupados. Linux utiliza un sistema de grupo privado de usuarios (UPG), tornando la administración mucho más sencilla. El sistema UPG no altera nada del patrón UNIX. Simplemente ofrece una nueva convención en la administración de grupos. Toda vez que se crea un nuevo usuario, automáticamente se crea un nuevo grupo. El sistema funciona de la siguiente forma:
Grupo de Usuario Privativo: Cada usuario tiene su propio grupo, del cual el es el único miembro. umask = 002: La máscara tradicional de usuario del Unix es 022, evita que otros usuarios y otros miembros del grupo modifiquen los archivos del usuario. Como cada usuario tiene su propio grupo, una umask igual a 002 evita que los usuarios modifiquen los archivos privativos del usuario. La umask reside en /etc/profile.
Bit SGID en Directorios: en el caso de que el bit SGID esté activo en un directorio (con el comando chmod g+s directorio), los archivos creados en el directorio tendrán el grupo del dueño igual al del directorio. Muchos administradores prefieren crear un grupo para cada proyecto y atribuyen el GID a cada usuario integrado al proyecto. Administrar archivos de la manera tradicional puede ser bastante exhaustivo, pues los archivos cuando creados por los usuarios pertenecen al grupo primario del usuario. Cuando la misma persona está alocada en diversos proyectos se crea una dificultad para compartir y administrar los archivos. Con el sistema UPG esta tarea se hace más sencilla.

2.6 seguridad en los archivos: varios elementos debe ser tenidos en cuenta para dar seguridad a los archivos, entre ellos cabría mencionar los siguientes:

- En una máquina configurada como estación de trabajo NO SE DEBE USAR NFS. Si es necesario, se debe asegurar de parchear convenientemente este paquete porque es fuente de numerosos problemas. El servidor NFS hace registro de todos los archivos montados en /etc/mtab. Si no hay más remedio que usar este servicio, se debe configurar lo más restrictivo posible.
- En el archivo /etc/exports se especifica a quién se exporta y cómo se exporta un sistema de archivos.
- Establecer en el /etc/profile el umask para los usuarios lo más restrictiva posible.
- No usar Samba. Si es necesario, se debe parchear convenientemente este paquete, porque es fuente de numerosos problemas.

- También se debe configurar lo más restrictivo posible el archivo /etc/smb.conf.
- Tener cuidado con los archivos .rhosts. Garantizan el acceso a la máquina sin autenticación. No es una alternativa segura Telnet. Es preferible usar como método de acceso un cliente ssh. Sobre todo, se debe revisar que no exista un archivo /root/.rhosts.
- Buscar todos los archivos SUID/SGID del sistema y monitorear los cambios en los mismos:
  root# find / -type f \(-perm -04000 -o -perm -02000 \)
- Son archivos especialmente explotados por intrusos potenciales. Todos aquellos archivos setuid root que no se usen, deben estar protegidos.

2.7 Configuración del inetd para evitar accesos del exterior Para evitar que accedan al equipo se puede configurar el demonio "inetd", que casi todas las distribuciones incluyen. Lo que hay que hacer es de lo más sencillo.

- Editar el archivo: /etc/hosts.deny
- Escribir dentro: ALL: ALL, Con lo cual nadie puede acceder a ningún servicio de tu equipo: Telnet, ftp, finger....
- Si quiere permitir estos servicios sólo a servidores locales, edita el archivo: /etc/hosts.allow
- Escribir dentro: ALL: LOCAL

Aunque claro.. Por lo visto hay un truco de "Hackers" que es simulare que tu dirección es una dirección local aunque entres desde el exterior. Para evitar esto... deberías poner en el /etc/hosts.deny: ALL: PARANOID

2.8 Logs son archivos donde el sistema registra todos los sucesos del sistema, desde una conexión por Telnet, o los archivos que un usuario se lleva o deja por ftp, hasta los intentos no válidos de login, intentos no válidos de su, etc. Hay que tener en cuenta que cuando un intruso se cuela en un sistema, lo primero que hace es modificar los logs para cubrir su rastro, por eso es importante revisarlos frecuentemente. Sin embargo mientas intenta entrar en la máquina deja rastros (que borrará una vez dentro), por eso es importante revisarlos periódicamente, para detectar intentos antes de que tengan éxito. Muchos fallos de login, por ejemplo, pueden indicar un intento de romper la seguridad del sistema. Lo que debe buscar en los registros dependerá de la distribución. En sistemas Linux que verifican el Estándar de Sistema de Archivos Linux ("Linux Filesystem Standard"), como RedHat, tendrás que mirar en /var/log. Una vez allí busca en messages, secure... y si se tienen servicios como samba, http, ftp... en los archivos donde estos registran los sucesos. Algo **muy importante** a la hora de revisar los logs es que la máquina tenga la hora correcta, ya que si tenemos que comparar con los logs de otras máquinas, si ambas no están sincronizadas será muy difícil. Para esto podemos usar NTP (Network Time Protocol) que sirve para poner en hora los computadores. Las distribuciones actuales de RedHat (desde las 5.0) contienen el software para usar NTP con lo que solo hay que configurarlo. Lamentablemente, todos estamos siempre muy ocupados y se nos olvida mirar los logs. Para automatizar esta tarea, se puede usar algún programa que nos resuma los logs y nos los mande por correo. Recomiendo el uso de *Logwatch* por su eficacia y facilidad de configuración. Logwatch lo que hace es que todos los días mira los logs, los resume en un informe y los puede guardar en un archivo o mandarlo por correo. Se puede configurar todo, desde cuando hace esto, el nivel de información que debe darnos en los logs, etc.

2.9 **Actualización** La mejor forma de no dar a los intrusos facilidades para entrar en los sistemas es estar actualizado con versiones nuevas. Normalmente cuando sale una nueva versión es por que la antigua tiene algunos errores, tanto de seguridad como de ejecución porque añade nuevas funcionalidades. En cualquier caso interesa instalarlo. Hay bases de datos inmensas en Internet con vulnerabilidades conocidas, organizadas por sistemas y cómo explotarlas. Si nuestro sistema es viejo y desactualizado, es una invitación a los intrusos para que se cuelen fácilmente. La actualización es algo que, al igual que la revisión de logs, es una tarea básica del administrador de todo sistema Linux (Unix).

2.10 Herramientas de administración Acceso Remoto Telnet es con mucho la herramienta remota más vieja y conocida, prácticamente cualquier versión de Unix viene con ella, incluso lo soportan sistemas como NT. Telnet sólo tiene uso cuando se administra el sistema desde modo comandos (algo para lo que NT no es tan bueno), lo cual lo convierte en perfecto para sistemas Unix. Telnet es increíblemente inseguro, las contraseñas y los nombres de usuarios, al igual que los datos de las sesiones vuelan en texto simple, siendo el objetivo preferido de los Sniffers. Telnet viene con todas las distribuciones de Linux. No deberías utilizar nunca el Telnet de fábrica para administrar remotamente un sistema.
SSL Telnet es Telnet con el añadido de cifrado SSL, lo cual lo hace bastante más seguro. Usando certificados X.509 (también conocidos como certificados personales) se pueden administrar sistemas con facilidad.
*SSH e*ra gratis al principio, pero ahora está bajo licencia comercial, sin embargo tiene numerosas características que lo hacen merecer la pena. Soporta diferentes tipos de autentificación (contraseña, basada en rhosts, llaves RSA), permite redireccionar puertos, y se puede configurar fácilmente a qué usuarios se les permite usarlo.
LSH es una implementación gratuita del protocolo SSH, LSH tiene licencia GNU y está empezando a perfilarse como la alternativa (comercialmente hablando) a SSH (que ya no es gratis). REXEC
REXEC es una de las utilidades UNIX más antiguas, permite ejecutar comandos en un sistema remoto, aunque tiene el serio problema de no tener un modelo de seguridad real. La seguridad se consigue mediante el uso de archivos 'rhosts', que especifican qué hosts/etc. pueden ejecutar comandos, lo cual está sujeto a Spoofing y otro tipo de explotadores. Jamás deberías utilizar el REXEC Standard para administrar un sistema.
Slush está basado en Open SSL, y actualmente soporta certificados X.509, lo cual, para grandes organizaciones, es una apuesta mucho mejor (y más sana) que intentar recordar varias docenas de contraseñas en diferentes servidores. Slush es GPL, pero todavía no está terminado (implementa la mayoría de la funcionalidad que se requiere para ser utilizable, pero tiene límites). Por otra parte, está completamente basado en software de código abierto, dejando pocas posibilidades a que pueda tener puertas traseras/etc. En último caso, podría reemplazar al SSH por algo mejor.
NSH es un producto comercial con todos sus detalles. Tiene soporte para cifrado, de modo que es relativamente seguro de usar. Es de una gran facilidad de uso, se hace un cd //nombredecomputador y con eso ya construye el log en ese computador, se puede copiar, modificar, etc. archivos con facilidad, ejecutar PS y ver la lista de procesos de ese computador, etc. NSH también dispone de un módulo Perl, lo cual hace sencilla la redacción de scripts de comandos, y es ideal para administrar muchos sistemas similares (como estaciones de trabajo). Además de eso, NSH está disponible en múltiples plataformas (Linux, BSD, Irix, etc.) con RPM's disponibles para sistemas Red Hat.
Fsh significa "Ejecución rápida de comandos remotos", y el concepto es similar al de rsh/rcp. Evita el costo de estar creando continuamente sesiones cifradas, habilitando un túnel cifrado utilizando ssh o lsh, y ejecutando todos los comandos sobre él.
secsh (Shell Seguro) aporta otra capa más de seguridad de login, una vez que has hecho log vía ssh o Telnet SSL pide otra contraseña, si introduce una errónea, secsh mata el intento de login.

2.11 Acceso Local
YaST (Yet Another Setup Tool) es un comando gráfico de líneas bastante interesante, que aporta una sencilla interfaz para la mayoría de las tareas administrativas. Sin embargo, no está pensado para limitar accesos a usuarios, así que sólo es útil para depurar errores y para permitir administrar el sistema a nuevos usuarios. Otro problema es que al contrario que Linuxconf, no está orientado a redes, lo cual quiere decir que hay que hacer un log en cada sistema que se desee manipular.
sudo le da a un usuario acceso setuid a un programa(s), se le puede especificar desde qué host(s) se les permite (o no) hacer login y tener acceso sudo (de modo que si alguien vulnera una cuenta pero está bloqueado, se minimizan los daños). Se puede especificar bajo qué usuario se ejecutará un comando, lo

cual da un grado de control relativamente preciso. Si tiene que dar acceso a los usuarios, debe asegurarse de especificar los hosts desde los que les está permitido hacer un login cuando estén utilizando sudo, de igual forma, da la ruta completa a los binarios, lo cual evitará problemas a la larga (p. ej. si le das acceso a "adduser" a un usuario, no hay nada que le impida editar su path y copiar bash a /tmp/adduser obteniendo el control de la máquina). Esta herramienta es muy similar a super pero con un control ligeramente inferior. Sudo te permite definir grupos de hosts, grupos de comandos, y grupos de usuarios, haciendo la administración más sencilla, a largo plazo.

Super es una de las pocas herramientas que se pueden utilizar hoy en día para dar a ciertos usuarios (y grupos) diferentes niveles de acceso a la administración del sistema. Además, se pueden especificar horas y permitir el acceso a scripts, puesto que da acceso setuid, incluso a comandos comunes, puede tener resultados inesperados (cualquier editor, cualquier herramienta de manipulación de archivos como chown, chmod, incluso herramientas como lp podrían comprometer partes del sistema). Debían viene con super, y existen rpm's disponibles en el directorio contrib. Es una herramienta potente (a veces deja a sudo a la altura del betún), pero necesita una sustancial cantidad de esfuerzo para implementarse correctamente (como cualquier herramienta potente).

Runas es muy parecido a sudo y Super, con algunas variaciones. Se crea un archivo de configuración listando el comando, como quién se ejecuta, y a qué usuarios/grupos/etc. se les permite ejecutarlo como tal. Además de esto, se pueden restringir el uso de opciones (argumentos), y se le puede solicitar al usuario el motivo (lo cual queda registrado con syslog). Esta es una buena característica, ya que con un poco de entrenamiento, se puede conseguir que el staff de administración documente lo que está haciendo de forma liviana

Webmin es (actualmente), una herramienta de administración no comercial. Es un conjunto de scripts de perl con un servidor WWW auto contenido al cual se accede utilizando un visor de WWW. Tiene módulos para la mayoría de las funciones de administración del sistema, aunque algunas son un poco temperamentales. Una de sus características más útiles es el hecho de que mantiene su propio usuario y contraseña para acceder a webmin, y se puede personalizar ya qué tiene acceso cada usuario (p. ej. usuario1 sólo puede administrar usuarios, usuario2 sólo puede reiniciar la máquina y usuario3 puede modificar la configuración del Apache).

Linuxconf es una herramienta de administración Linux de propósito general, que se puede utilizar desde la línea de comandos, desde X, o vía su propio servidor WWW. Es una de las mejores herramientas para administración automatizada del sistema, ya que es relativamente ligera desde la línea de comandos (en realidad está dividida en varios módulos). Desde X proporciona una vista general de todo aquello que puede configurarse (PPP, usuarios, discos, etc.). Para utilizarlo vía visor WWW, primero hay que ejecutar Linuxconf en la máquina y añadir el o los hosts o red(es) a las que quieres permitir conectarse (Conf> Misc> Linuxconf network access), salvar los cambios y salir. Luego, cuando te conectes a la máquina (por defecto Linuxconf sólo acepta root como la cuenta, y Linuxconf no soporta ningún tipo de cifrado (se ejecuta independientemente en el puerto 901), de modo que no es aconsejable la utilización de esta característica entre redes, a menos que se tenga IPSec o algún otro tipo de nivel de seguridad IP.

Coas El proyecto COAS (Caldera Open Administration System) es un proyecto muy ambicioso para proporcionar un marco abierto de administración de sistemas, desde línea de comandos (con interfaz semi-gráfico), desde X (utilizando el componente qt) hasta el web. Hace una abstracción de los datos reales de configuración aportando una capa intermedia, permitiendo de esta forma su uso en variadas plataformas Linux.

2.12 Otras herramientas basadas en red Virtual Network Computer (VNC) es parecido a PCAnywhere. Se puede mostrar un escritorio gráfico, y controlarlo remotamente, con NT o Linux como servidor y/o cliente. El VNC es bastante bueno a través de una Ethernet de 10 megabit, sin embargo tiende a utilizar un montón de potencia computacional relativamente comparado con otros métodos de administración remota. La seguridad del VNC no es tan buena, pero hay varios sitios con información acerca de asegurar VNC, utilizando SSL, SSH y otros métodos. MindVNC es un cliente java que utiliza SSH.

2.13 Detección de intrusos mediante análisis de huellas entre los archivos que guardan registros cabe mencionar:

Utmp: Guarda un registro (Log) de los usuarios que están utilizando el sistema mientras están conectados al mismo. Directorios: /var/adm/utmp y /etc/utmp

Bibliografía

Bruce Scheneier. Secret & Lies John Wiley & Sons, 2000

Gerald L. Kovacich & William C. Boni. High Technology Crime Investigator Handbooks. Butterworth Heinemann, 1999

Harry Newton. Newton's Telecom Dictionary 17th edition. CMP Books. February 2001

Tere Parnell. Redes de Area Extensa. Mc Graw-Hill, 1997

Darren L. Spohn. Data Network Design 2nd Edition. Mc Grawn-Hill, 1997

Data and Computer Communications 6th edition. William Stalling. Wiley & Sons, 2000, 2000

Wireless Communicatios and Networks. William Stalling. Prentice Hall, 2002

Computer Networks 3rd edition. Andrew Tanembaum. Prentice Hall, 1996

Cisco Secure Internet Security Solution. Andrew G. Mason, Mark Newcomb. Cisco Press, 2001

Information Technology Audit Handbook. Doug Dayton. Prentice Hall, 1997

Interconnections 2nd Edition, Radia Perlman. Addison Wesley, 2001

Information Systems Control and Audit. Ron Weber. Prentice Hall, 1998

MCSE Window 2000 Network Security Design. Gary Govanus & Robert King. Sibex, 1999

Network and Internetwork Security. William Stallings. Prentice Hall, 1995

Fighting Computer Crime. Donn B. Parker. Wiley & Sons, 1998

TCP/IP 3rd edición. Douglas E. Comer. Prentice Hall, 1996

Computer Security Basics. Deborah Rusell, G. T. Gangemi. O´Reilly & Associates,1991

Information Warfare and security. Dorothy E. Denning. Addison Wesley, 1999

Handbook of Information Security Management. Micki Krause, Harold F. Tipton. Auerbach,1999

Building Internet Firewalls. D. Brent Chapman, Elizabeth D. Zwicky. O´Reilly & Associates,1995

Computer Security. Dieter Gollmann. Addison Wesley, 1999

Disaster Planning and Recovery. Alan M. Levitt. Prentice Hall, 1997

Internet & TCP/IP Network Security. Uday Pabrai, Vigía Gurbani. Mc Grawn-Hill, 1996

Fundamentals of Risk Analysis and Risk Management. Vlasta Molak. Lewis Publishers, 1997

Mastering Network Security. Chris Brenton. Sybex, 1999

Intrusion Detection. Terry Escamilla. Wiley & Sons, 1998

Linux Security. Bob Toxen. Prentice Hall, 2001

Linux máxima seguridad. Varios. Prentice Hall, 2001

Hackers. Joel Scambray, Stuart Mc Clure, George Kurtz, Mc Graw-Hill, 2001

The Essential guide to Telecommunications. Annabel Z. Dodd. Prentice Hall, 1999

Internet Connections Over Cable. Mark E. Laubach, David J.

Farber, Stephen D. Dukes. Wiley & Sons, 2001
Acceptable Risks. Larry Heimann. Michigan University, 2000
Hack Attacks Revealed. John Chirillo. Wiley & Sons, 2001
Network Auditing. Gordon E. Smith. Wiley & Sons, 1999