UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERÍA.
Postgrado en Sistemas de Información

Trabajo de Grado de Especialista

ESTABLECIMIENTO DE UN SISTEMA DE SEGURIDAD PARA LAS ORGANIZACIONES BANCARIAS PRIVADAS.

Presentado por
Mayo Villegas, Robinson José;
para optar al título de
Especialista en Sistemas de Información

Tutor
Manuel Gaspar

Caracas, Enero del 2008

DEDICATORIA

A mis Hijos, que son la Luz, el Norte y sobre todo el Motivo Principal de mi lucha por la superación continua como persona y profesional.

A la Universidad Católica “Andrés Bellos” por brindarnos la oportunidad de superarnos personal y profesionalmente.

A los profesores de este cohorte por su dedicación y empeño a enseñarnos, y muy especialmente al profesor Manuel Gaspar mi tutor Académico.

Tabla de Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRAFICOS

INTRODUCCIÓN

Hoy en día, tal como lo plantea la Norma ISO 27001, la información es uno de los objetos de mayor valor para las empresas. La seguridad de información tiene como propósito proteger los activos de información (la información en sí, los equipos que la soportan y las personas que la utilizan), independientemente del lugar que se localice, en base a la preservación de tres principios básicos: disponibilidad, confidencialidad e integridad. Estos principios están presentes desde tiempos antiguos, pero hoy ,donde la tecnología de información se encuentra en casi todas las actividades empresariales o particulares del ser humano, la seguridad de la información ha tomado un lugar importante dentro del mundo cibernético.

En base al tema de la seguridad de información nos encontramos entre realidades y mitos. Lo que ha ocasionado ver a la tecnología de información como una herramienta peligrosa para los usuarios, donde existen seres que desean hacer el mal (hacker) y otro grupo buscando la forma de proteger los activos de información. En otros casos las organizaciones han creado estructuras de hardware y software que no están acordes con sus necesidades, pero también tenemos gerentes de organizaciones que suponen que la seguridad de información es una moda y que ellos no están expuestos a ningún tipo de riesgo.

Es tan importante el tema de seguridad de la información que países y organizaciones mundiales han tenido que crear leyes, normas o acuerdos, para tener marcos jurídicos sobre el tema. De esta forma, poder hacer frente a los desafíos (hacker, delitos informáticos, uso indebido de la información...) que la era de las telecomunicaciones y el uso de la Internet han derivado.

Las instituciones financieras privadas en Venezuela, específicamente la banca, posee un esquema de funcionamiento bastante homogéneo, prestan de manera similar los mismos servicios utilizando canales de distribución análogos (red de agencias o sucursales, Internet, banca en línea, centro de llamadas, conexión con los entes reguladores, etc.). Bajo esta premisa, podemos establecer una estructura o un sistema de seguridad (software, hardware, procedimientos y políticas), que pueda ser utilizado por las instituciones privadas que conforman el sistema financiero venezolano.

Es importante tener presente que los modelos o mecanismos de seguridad ofrecen una robustez relativamente segura para un período de tiempo determinado, ya que la aparición de nuevas brechas de seguridad obligan a la constante revisión y ajuste de la

infraestructura de seguridad, motivo por el cual la gestión de seguridad de datos, es una tarea cotidiana. El esquema o estructura de seguridad sugerido en este trabajo está orientado hacia las instituciones bancarias del sector privado.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

La seguridad de activos de información ha comenzado a tomar un lugar determinante en el mundo de los negocios, en particular en la gestión integral de riesgo, y se ha convertido en un elemento fundamental a ser considerado en toda estrategia organizacional con miras a lograr metas de negocio importantes a corto, mediano y largo plazo. Las instituciones financieras no son ajenas a este proceso y ahora que la totalidad de ellas han tenido que abrir sus sistemas de información producto de la masificación de Internet como canal de venta de productos y servicios. Por ejemplo, Home-Banking (banca electrónica), B2B (negocio electrónico con negocio electrónico), B2C (negocio electrónico con comercio electrónico), etc.

Las organizaciones experimentan la necesidad de definir estrategias efectivas que faciliten una gestión segura de los procesos del negocio, con el fin de darle mayor resguardo a la información y al mismo tiempo, adaptarse a los continuos cambios de la organización como consecuencia de las exigencias del mercado y el Estado Venezolano.

Tal necesidad ha impulsado a la eliminación de viejos paradigmas, como por ejemplo que algunos ejecutivos y tecnólogos perciben la seguridad de activos de información como un asunto meramente técnico que debe ser resuelto mediante la utilización de un componente tecnológico en particular. Sin embargo, existen interrogantes relacionadas con la manera de aplicar los nuevos conceptos, sin que éstos impacten de manera significativa en las operaciones de una organización, y que además perduren en el tiempo.

Para alcanzar la excelencia que muchas de las organizaciones están buscando en materia de seguridad de activos de información, algunos ejecutivos así como profesionales de tecnología de información, (TI), están haciendo un esfuerzo para organizar de forma adecuada sus recursos, basados en su entendimiento de la seguridad de activos de información. Este entendimiento, permite darle respuesta a una serie de interrogantes que resultan relevantes:

1) Desde una perspectiva tecnológica. ¿Qué elementos de TI requiere mi empresa para satisfacer las necesidades de integridad, disponibilidad, confidencialidad y auditabilidad de los activos de información?

2) Desde una perspectiva de recursos. ¿Cómo identifico la combinación adecuada de personal, procesos y tecnología necesarios para mantener y optimizar la seguridad de activos de información?

3) Desde una perspectiva estratégica. ¿Está alineada la estrategia de seguridad de activos de información con la estrategia del negocio y el ambiente de riesgo?

4) Desde una perspectiva de control. ¿Dónde reside la responsabilidad de la seguridad de activos de información en la organización?

5) Desde una perspectiva de gestión. ¿Cómo administro la seguridad de activos de información en conjunto con: las necesidades del negocio, los constantes cambios de TI y las regulaciones actuales?

6) Desde una perspectiva de costo. ¿Cuál es el costo de los activos de información a proteger?. ¿Cuál es el costo de la inversión en seguridad de datos?

Asimismo, existe una creciente necesidad en las organizaciones en cuanto a los servicios de seguridad de activos de información, proporcionados internamente o por terceras partes que garanticen la existencia de controles adecuados.

Para muchas organizaciones, la información y la tecnología, representan uno de sus activos más valiosos, debido a:

1) La creciente dependencia en la información, en los sistemas y las aplicaciones.

2) El incremento de las vulnerabilidades y una diversidad de amenazas, tales como “la guerra de información” y las “ciber-amenazas” que ponen en riesgo el (los) sistema(s) que soporta(n) el negocio.

3) El costo en las inversiones actuales y futuras en TI.

4) El potencial que tiene la TI para cambiar radicalmente las organizaciones; los procesos de negocio; el aprovechamiento de nuevas oportunidades y la reducción en los costos.

5) La existencia de un contexto de mayor sofisticación en la operatividad de las empresas, con un escenario de tendencias de control de riesgo operacional.

6) Nuevas regulaciones en materia de control, como por ejemplo: la ley Estadounidense Sarbanes-Oxley, y las más recientes resoluciones de los organismos reguladores de los diversos sectores en el país. Para el caso de las organizaciones Financieras, la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN) prohibió el almacenamiento y procesamiento de información fuera del País. Esta misma Superintendencia en fecha 29 de mayo del año 2003, mediante la resolución 136.03 que tiene como base los principios del Nuevo Acuerdo de Capital

conocido como Basilea II, realiza una serie de exigencias sobre las instituciones financieras para el manejo de los riesgos a las cuales están sometidas las organizaciones.

Adicionalmente fueron promulgadas durante el año 2001 la Ley de Delitos Informáticos y La Ley de Mensajes de Datos y Firmas Electrónicas.

Uno de los factores críticos de éxito es comprender que el asegurar o proteger los activos de información, no es un problema exclusivamente de la TI, sino de conocer cuáles son los objetivos e iniciativas del negocio y de qué forma la seguridad de activos de información va a propiciar el logro de los mismos. Ninguna empresa o corporación opera en un ambiente libre de riesgo. Es importante acotar que la sola existencia de la unidad de seguridad de datos no crea un ambiente libre de riesgos.

En consecuencia, ahora son mayores las amenazas a las cuales las organizaciones están expuestas, que van desde virus informáticos hasta el espionaje corporativo, y que encuentran nuevas posibilidades de atentar contra la seguridad de la información. Esta situación ha creado preocupación en los entes reguladores, y ha llevado a las organizaciones a tomar posturas más activas, trayendo consigo la creación de unidades especializadas en la gestión de los riegos informáticos, como lo es la organización del departamento de seguridad de datos.

JUSTIFICACIÓN

En la actualidad, cada vez son mayores las inversiones que realizan las empresas en la compra de productos, sino que comienzan a dotar parte de su presupuesto para destinarlo a la gestión de la seguridad de la información. El concepto de seguridad ha variado, acuñándose un nuevo concepto: “seguridad gestionada”, que ha desbancado al de “seguridad informática”. Las medidas que comienzan a tomar las empresas giran entorno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes: técnica, legal y organizativa, es decir un planteamiento coherente de directrices, procedimientos y criterios que permiten desde la dirección de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de Información, la organización afín y sus infraestructuras. Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental la cual reza como sigue: “la seguridad absoluta no existe”. Tomando como referencia esta máxima, una entidad puede adoptar alguna de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información. El presente trabajo recoge las mejores practicas que pueden ser utilizadas por las organizaciones financieras venezolanas para establecer un ambiente computacional lo razonablemente robusto.

Dentro de la amplia gama de productos o soluciones de seguridad muchas no cumplen o son aplicadas a las organizaciones financieras, motivo por el cual esta guía de referencia permitirá escoger la solución más óptima para la brecha de seguridad, la cual puede ser aplicada de acuerdo a las necesidades de la organización.

OBJETIVOS GENERALES

Proponer un compendio de medidas o mecanismos necesarios para la construcción de una infraestructura tecnológica razonablemente segura en lo concerniente a confidencialidad, disponibilidad, consistencia y auditabilidad dentro de la organización bancaria en la República Bolivariana de Venezuela

OBJETIVOS ESPECIFICOS

1) Sugerir cuales mecanismos de seguridad son apropiados para la protección de la información contenida en los sitios Web de las instituciones financieras.
2) Proponer la estructura y ubicación de la gerencia de seguridad de datos dentro de las organizaciones.
3) Documentar cuales mecanismos de seguridad son apropiados para la protección de la información de las amenazas internas.
4) Documentar y proponer una serie de políticas y normas orientadas a la protección de los activos de información.

CAPITULO II

ANTECEDENTES

El problema de la seguridad de la información no es nuevo. Desde las antiguas civilizaciones hasta la era digital, los mensajes cifrados han representado un papel destacado en la vida del hombre, haciendo gala de su ingenio para garantizar la confidencialidad de sus comunicaciones. La primera medida de seguridad conocida es la utilización de los criptogramas. “La criptografía, etimológicamente del griego kryptos "escondido" y graphein "escribir", no es más que arte de enmascarar los mensajes con signos convencionales que sólo cobran sentido a la luz de una clave secreta. Sus rastros se encuentran en las tablas cuneiformes y en los papiros que demuestran que las primeras civilizaciones (egipcios, hebreos, babilonios y asirios) conocieron y aplicaron sus inescrutables técnicas que alcanzan hoy su máxima expresión gracias al desarrollo de los sistemas informáticos y de las redes mundiales de comunicación”.[1]

El primer manual sobre la materia surgió en la Europa de la Edad Media, impulsada por las intrigas del papado y las ciudades-estado italianas; Grabiele de Lavinde, un servidor del Papa Clemente VII fue quien escribió dicho manual.

En 1466, León Battista Alberti, concibió el sistema poli-alfabético el cual emplea varios abecedarios, saltando de uno a otro cada tres o cuatro palabras. El emisor y el destinatario han de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos que determinaría la correspondencia de signos.

Un siglo después, Giovan Battista Belaso de Brescia instituyó una nueva técnica **“**La clave” que formada por una palabra o una frase, debe transcribirse letra a letra sobre el texto original. Cada letra del texto se cambia por la correspondiente en el alfabeto que comienza en la letra clave.

Los métodos clásicos distan mucho de ser infalibles. En algunos casos, basta hacer un simple cálculo para desentrañar los mensajes ocultos.

Retomando el concepto de las ruedas concéntricas de Alberti, a principios del siglo XX se diseñarón los teletipos equipados con una secuencia de rotores móviles; éstos giraban con cada tecla que se pulsaba, revolucionando la criptografía. De esta forma, en lugar de la letra elegida, aparecía un signo escogido por la máquina según las diferentes reglas en un código poli-alfabético complejo, de ello surgen los aparatos que

[1] http://Introducción a la criptografía

se llamaron traductores mecánicos. “Unos de los predecesores de los traductores mecánicos fue la Rueda de Jefferson, el aparato mecánico criptográfico más antiguo que se conserva y cuya patente data de 1919. Obra del holandés Alexander Koch, quien comparte honores con el alemán Arthur Scherbius, el inventor del Enigma, una máquina criptográfica que los nazis creyeron inviolable sin saber que a partir de 1942 propiciaría su derrota cuando los aliados fueron capaces de descifrar todos los mensajes secretos alemanes.”[2]

Los códigos de la versión japonesa de Enigma, llamados Purple-violeta, se descifraron en el atolón de Midway, cuando un grupo de analistas dirigidos por el comandante Joseph J. Rochefort, descubrió que los nipones señalaban con las siglas AF su objetivo. Para comprobarlo, Rochefort les hizo llegar este mensaje: "En Midway se han quedado sin instalaciones de desalinización". Inmediatamente, los japoneses la retransmitieron en código: "No hay agua potable en AF" de forma tal que el almirante Nimitz consiguió una clamorosa victoria, hundiendo cuatro portaviones japoneses en Midway.

“Mientras los nazis diseñaron Enigma para actuar en el campo de batalla, los estadounidenses utilizaron un modelo llamado Sigaba y apodado por los alemanes como "la gran máquina". Este modelo funcionó en estaciones fijas y fue el único artefacto criptográfico que conservó intactos todos sus secretos durante la guerra. Alertado por las posibilidades que las innovaciones tecnológicas abrían, el gobierno estadounidense, intentó en los años cincuenta la introducción de la Data Encryption Standard (DES), un sistema desarrollado por la National Security Agency (NSA)”[3]. El objetivo era que todos los mensajes cifrados utilizaran el DES; un intento de control que pocos aceptaron. Finalizada la contienda, las nuevas tecnologías electrónica y digital se adaptaron a las máquinas criptográficas, se dieron así los primeros pasos hacia los sistemas criptográficos actuales, mucho más fiables.

Sin embargo, “Philip Zimmermann, un criptógrafo aficionado, levantó hace unos años las iras del gobierno estadounidense. Su delito fue idear un sistema de codificación aparentemente inviolable, el Pretty Good Privacy (PGP) distribuido por las redes de comunicación para que cualquiera pudiera utilizarlo”[4]. Algo que no podía agradar a

[2] Introducción a la criptografía (Trabajo citado 1).
[3] Introducción a la criptografía (Trabajo citado 1).
[4] Philip R. Zimmermann es el creador de Pretty Good Privacy

quienes ven en la criptografía un arma de doble filo, útil para los gobiernos y funesta en manos de terroristas y delincuentes.

Con la expansión de la red se ha acelerado el desarrollo de las técnicas de ocultación, ya que al ritmo que crece la libertad de comunicación, se multiplican los riesgos para la privacidad.

Hoy por hoy, la seguridad va más allá de los procesos de criptografía. Cuando hablamos de seguridad de datos nos referimos a los activos de información y a los equipos informáticos como unos de los recursos más importantes y vitales para las organizaciones, pues sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón su preservación, utilización y mejoramiento son claves para la continuidad del mismo. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales. El costo operacional de un día de inactividad puede calcularse, pero ¿qué ocurriría si la información que otros han encomendado a la empresa es puesta en peligro públicamente? Una brecha de seguridad corporativa y la consiguiente pérdida de credibilidad antes los clientes, proveedores y el gobierno pueden arriesgar la propia naturaleza de la empresa o su continuidad operativa. Las empresas que no realizan una gestión pro-activa como parte de su estrategia de seguridad de TI poseen más disposición a los riesgos informáticos.

"Los virus y gusanos explotan vulnerabilidades de seguridad del software para atacar y lanzar nuevos ataques. Estas vulnerabilidades dan a los atacantes la oportunidad de poner en peligro la información e impedir los accesos a los usuarios validos, habilitando los privilegios escalados y exponiendo los datos a visiones o manipulaciones no autorizadas"[5].

Recientemente la empresa Espiñeira, Sheldon y Asociados, firma miembro de Price Water House Coopers, llevó a cabo un estudio en más de 200 empresas venezolanas para determinar el grado de compromiso de la alta gerencia con el tema de seguridad.

Durante una presentación titulada "De la integración vendrá la innovación[6]" en donde se expuso, 1) cómo la construcción de una infraestructura segura es

[5] www. Enciclopedia de Virus. Virus informático desde la A-Z
[6] www. Revista PC-News.com

probablemente una de las principales prioridades y uno de los desafíos más importantes para las organizaciones; 2) se hizo referencia a distintos temas que actualmente preocupan a las compañías como la relación entre seguridad, privacidad y los temas regulatorios; 3) Cómo una visión innovadora de la administración de los sistemas y de la seguridad informática puede ofrecer la integración para asegurar una protección efectiva.

Por su parte la empresa Microsoft realizo para América Latina, un curso para especialistas de seguridad vía Web, cuyo objetivo no es otro que la formación integral de personas para el manejo de soluciones con sus herramientas. Este tipo de iniciativas está siendo implementadas por otros fabricantes de tecnologías de información, donde el concepto de seguridad puede ser un punto de diferenciación con sus competidores.

MARCO TEORICO

La seguridad de la información puede ser vista desde su rol estratégico en los procesos de negocio, al identificar con qué recursos (organización, procesos, tecnología), se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. En este sentido, la seguridad de la información es un aspecto sumamente importante en la relación que se establece entre el negocio, sus clientes, socios, proveedores y empleados.

Como un proceso estratégico, la seguridad de la información está enfocada en proteger los activos de información de una organización contra pérdidas o uso indebido, o focalizada a brindar acceso a los activos de información apoyando los objetivos de negocio. Uniendo estos dos conceptos – seguridad como "protección" y seguridad como "habilitador de accesos" – se define de manera integral un nuevo enfoque de Seguridad de la Información en las organizaciones.

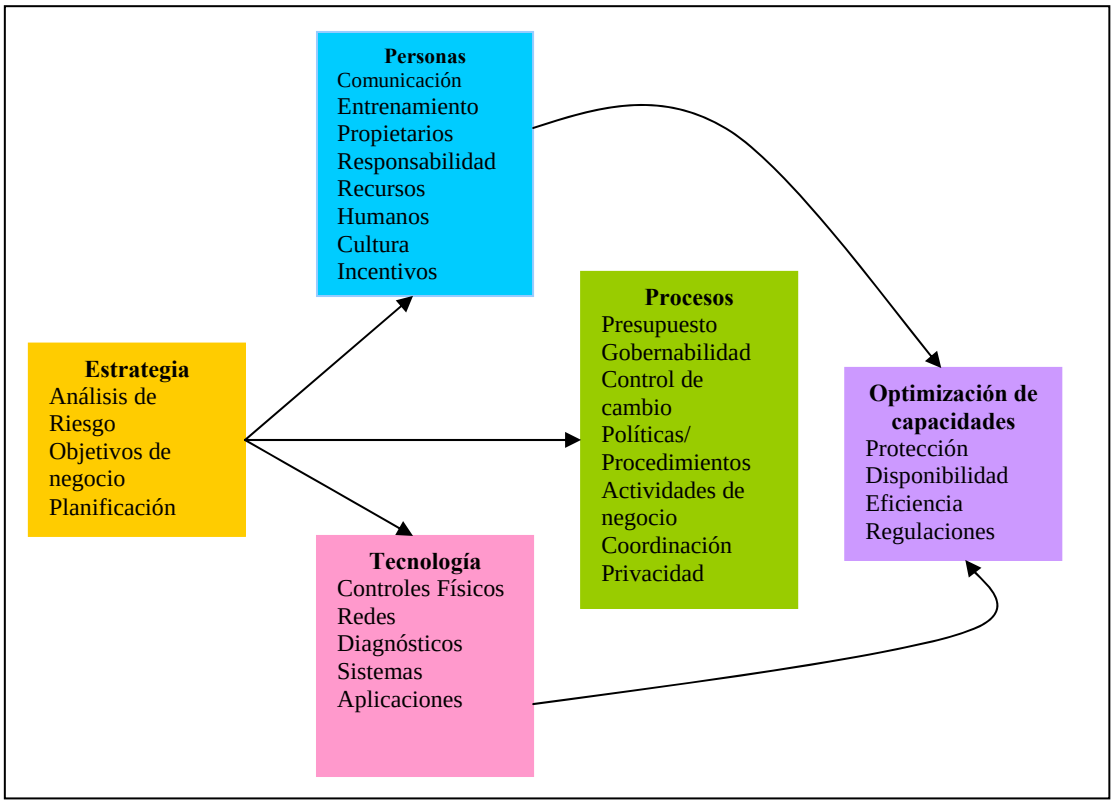
"La seguridad de la información hoy día no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología "(Ver Figura 1, "Seguridad de la Información" tomada de la presentación de Espiñeira, Sheldon y Asociados)"[7]. Si no se cuenta con reglas, lineamientos, responsabilidades y procedimientos predefinidos, y ante la ausencia de personal que es capacitado para la gestión del proceso, la inversión en tecnología solamente no es más que una pérdida de dinero"[8]. Este concepto de seguridad de la información como una solución integral es esencial para la transformación de este nuevo enfoque, en una plataforma tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para el negocio.

A medida que el rol de seguridad de la información evoluciona, los directivos y ejecutivos de negocio reconocen que éste es sin duda el primer paso en la relación entre la organización, sus clientes, socios de negocio, proveedores y empleados. En este sentido, la Seguridad de la Información acarrea enormes implicaciones para las organizaciones debido a que la confianza es la base para el intercambio, y su ausencia es una buena razón para hacer negocios con la competencia.

---

[7] www. Revista.Pc-News.com
[8] Revista citada (PC-News.com , cita número 7).

Figura 1 "Seguridad de la Información"[9]



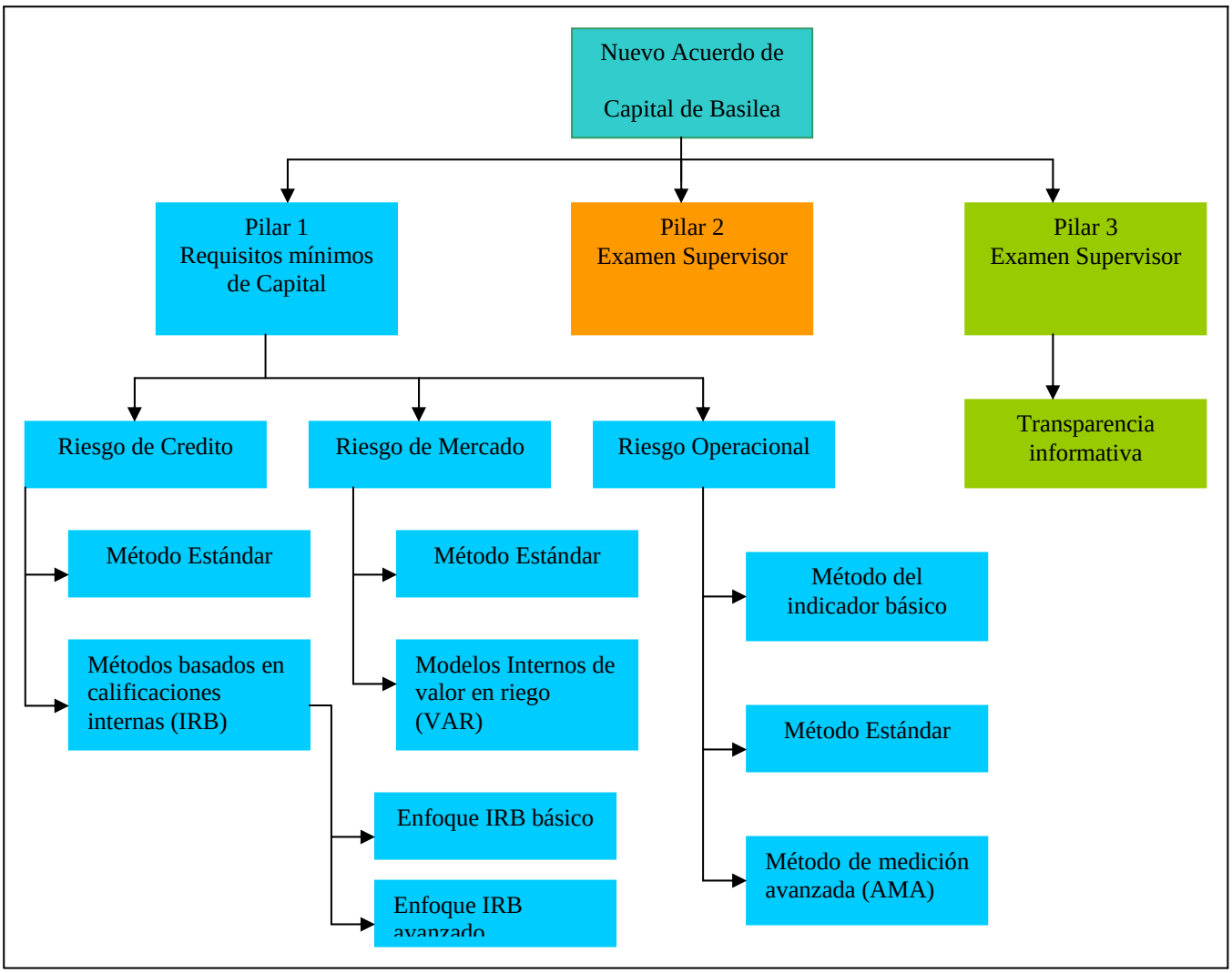
Dentro del mundo de la seguridad de la información es necesario hacer referencia a la Resolución 136.03 de la SUDEBAN (Superintendecia de Bancos y otras Instituciones Financieras) que tiene como base los acuerdos de Basilea II.

¿Que es el Comité de Basilea? "El Comité de Basilea fue creado en 1974 por los presidentes de los bancos centrales del Grupo de los 10 - G10, hoy día los países que lo integran están representados por sus bancos centrales; así como, las instituciones que formalmente detentan la responsabilidad de actuar como supervisores bancarios. En este comité se elaboran pautas sobre estándares de supervisión, lineamientos y recomendaciones sobre prácticas bancarias, a fin de ser adoptados por los entes supervisores de acuerdo a las necesidades locales"[10]. El Comité de Basilea de Supervisión Bancaria pública el Acuerdo de Capital de Basilea (Basilea I), el primer acuerdo internacional para lograr una convergencia y homogeneidad en la forma de medir la adecuación de capital en los Bancos y en el 2.001 se publica una propuesta consultiva para un Nuevo Acuerdo de Capital de Basilea (Basilea II).

[9] Revista citada (PC-News.com , cita número 7
[10] Oracle-HP-Deloitte, Basilea II, Adaptar, Adoptar o Peder.

Basilea II propone establecer una relación directa entre el requerimiento de capital de un Banco y el grado de riesgo en que éste incurra. A continuación se describen los 3 pilares:

Figura 2 “Los tres pilares de Basilea II”[11]



Pilar 1: Requerimientos Mínimos de Capital; define nuevas reglas para el tratamiento del riesgo de crédito, definiendo tres opciones distintas para el cálculo del Riesgo de Crédito y fija, por primera vez, requisitos de capital por riesgo operacional. El riesgo de mercado no sufre cambios significativos en relación con la enmienda al Acuerdo de Capital de 1996 (Basilea I).

Pilar 2: Examen Supervisor; apunta a la necesidad de los bancos de evaluar sus posiciones de suficiencia de capital con respecto a sus riesgos globales, así como la de

[11]Referencia citada numero 10

los supervisores para examinar y adoptar las medidas adecuadas como respuestas a dichas evaluaciones.

Pilar 3: Disciplina de Mercado; establece la obligación de la transparencia informativa sobre el perfil de riesgo de las instituciones financieras y sobre su nivel de capitalización. “En este contexto, Basilea II constituye una base fundamental de conocimientos que apoya, con mejores prácticas y criterios uniformes recogidas en más de 500 páginas, el desarrollo de aspectos organizativos, políticas, procedimientos y modelos tanto cualitativos como cuantitativos avanzados para la gestión de los riesgos de crédito, de mercado y operacional”[12], en la Figura No 3 se muestran diversos “métodos de gestión de riesgos propuestos por Basilea II”[13].

Figura 3 Métodos de gestión de riesgos

Dentro de este marco, el riesgo operativo, es el riesgo de que deficiencias en los sistemas de información o controles internos produzcan pérdidas inesperadas, este tipo de riesgo por lo general está asociado a errores humanos, fallas en los sistemas y a la existencia de procedimientos y controles. La Superintendencia de Bancos y Otras Instituciones Financieras define al riesgo operacional como: "La posibilidad de daños potenciales y pérdidas motivados a las formas de organización y a la estructura de sus

[12] Banco Nacional de Crédito – Unidad de Administración Integral de Riesgo
[13] Obra citada numero 10.

procesos de gestión, debilidades en los controles internos, errores en el procesamiento de operaciones, fallas de seguridad e inexistencia o desactualización en los planes de contingencia del negocio. Así como, la potencialidad de sufrir pérdidas inesperadas por sistemas inadecuados, fallas administrativas, eventos externos, deficiencias en controles internos y sistemas de información originadas, entre otros, por errores humanos, fraudes, incapacidad para responder de manera oportuna o hacer que los intereses de la Institución se vean comprometidos de alguna u otra manera".

Una vez detectado el riesgo la institución deberá "cuantificarlo". La cuantificación del riesgo operacional, consiste en la medición de las pérdidas originadas por actividades, áreas o procesos internos, a los fines de contar con registros históricos que permitan determinar áreas o procesos con mayor susceptibilidad a la generación de pérdidas y así desarrollar mecanismos o medidas que minimicen los factores que ocasionan la materialización de tales riesgos.

Por último la SUDEBAN en su resolución 136.03 regula al Sistema Bancario Nacional a que se implementen procedimientos de evaluación acerca de la correcta interacción de los procesos, actividades, sistemas y prácticas utilizadas en las áreas operativas y administrativas a los fines de controlar situaciones o condiciones que puedan derivar en pérdidas o inadecuadas asignaciones de recursos. Igualmente, se implementarán mediciones de pérdidas que se originen por actividades, áreas o procesos internos, a los fines de contar con registros históricos que permitan determinar susceptibilidades

El marco que se detalla a continuación presenta tres métodos para calcular los requerimientos de capital por riesgo operativo. En orden creciente de sofisticación y sensibilidad al riesgo, estos métodos son: (1) el Método del Indicador Básico; (2) el Método Estándar y (3) los Métodos de Medición Avanzada (AMA).

Se insta a los bancos a ir progresando a lo largo de la gama de métodos disponibles a medida que desarrollen sistemas y prácticas de medición más sofisticados para el riesgo operativo. “Los bancos con presencia internacional y los bancos con una exposición importante al riesgo operativo (por ejemplo, los bancos especializados) deberían utilizar un método más sofisticado que el Método del Indicador Básico que resulte adecuado al perfil de riesgo de la institución”[14].

[14] Normas para una Adecuada Administración Integral de Riesgos; Superintendencia de Bancos y Otras Instituciones Financieras, Resolución Bancaria 136.03 publicada el 3 de Junio de 2003 en la Gaceta Oficial N° 37.703

Se permitirá a los bancos utilizar el Método del Indicador Básico o el Método Estándar en parte de sus actividades y un AMA en otras operaciones, siempre que se satisfagan ciertos criterios mínimos.

Salvo que cuente con la aprobación del regulador (SUDEBAN), no se permitirá que un banco vuelva a utilizar un método más sencillo una vez que se le haya autorizado a utilizar un método más avanzado. Ahora bien, en caso de que el regulador determine que un banco que utiliza un método más avanzado ha dejado de satisfacer los criterios de admisión para dicho método, podrá exigirle que vuelva a emplear un método más sencillo en todas o en parte de sus operaciones, hasta que cumpla las condiciones estipuladas por el regulador para poder volver al método más avanzado.

El Método del Indicador Básico

Los bancos que utilicen el Método del Indicador Básico deberán cubrir el riesgo operativo con un capital equivalente al promedio de los tres últimos años de un porcentaje fijo (denotado como alfa) de sus ingresos brutos anuales positivos. Al calcular este promedio, se excluirán tanto del numerador como del denominador los datos de cualquier año en el que el ingreso bruto anual haya sido negativo o igual a cero.

Método del Indicador Básico

Capital de Riesgo Operacional = Ingreso Bruto X α

α es un porcentaje determinado por el regulador *

El Método Estándar

En el Método Estándar, las actividades de los bancos se dividen en ocho líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista. El ingreso bruto de cada línea de negocio es un indicador amplio que permite aproximar el volumen de operaciones del banco y, con ello, el nivel del riesgo operativo que es probable que asuma el banco en estas líneas de negocio. El requerimiento de capital de cada línea de negocio se calcula multiplicando el ingreso bruto por un factor (denominado beta) que se asigna a cada una de las líneas. Beta se utiliza como una aproximación a la relación que existe en el conjunto del sector bancario entre el historial

de pérdidas debido al riesgo operativo de cada línea de negocio y el nivel agregado de ingresos brutos generados por esa misma línea de negocio.

Cabe mencionar que, en el Método Estándar, se calcula el ingreso bruto de cada línea de negocio y no el obtenido por la institución en su conjunto. Así, por ejemplo, en finanzas corporativas, el indicador es el ingreso bruto generado por la línea de negocio de finanzas corporativas.

La exigencia total de capital se calcula como la media de tres años de la suma simple de las exigencias de capital regulador en cada una de las líneas de negocio cada año. Para un año dado, los requerimientos de capital negativos (resultantes de ingresos brutos negativos) en cualquiera de las líneas de negocio podrán compensar los requerimientos positivos en otras líneas de negocio sin límite alguno.

Método Estándar

Capital de Riesgo Operacional = Ingreso bruto por línea de negocio X β

â es un porcentaje determinado por el regulador *

El Método AMA (Método avanzado)

En los AMA, el requerimiento de capital regulador será igual a la medida de riesgo generada por el sistema interno del banco para el cálculo del riesgo operativo utilizando los criterios cuantitativos y cualitativos aplicables a los AMA que se analizan más adelante. La utilización de los AMA están sujeta a la aprobación del supervisor (SUDEBAN).

Los bancos que adopten los AMA, previa aprobación de la SUDEBAN, podrán utilizar un mecanismo de distribución a efectos de determinar el requerimiento de capital regulador para filiales de bancos con actividad internacional que no se consideran significativas con respecto al grupo en su conjunto pero que están sujetas al presente Marco en virtud del Primer Pilar. El consentimiento del regulador podrá depender de que el banco demuestre a los supervisores oportunos que el mecanismo de distribución entre estas filiales es el adecuado y se apoya en datos empíricos. El consejo de administración y la alta dirección de cada filial deberán realizar su propia evaluación de los riesgos operativos de la misma; así como, controlar y asegurar que el capital que mantiene es el adecuado para estos riesgos.

Sujeto a la aprobación del supervisor, la incorporación de una adecuada estimación de los beneficios de la diversificación deberá realizarse para el grupo en general así como al nivel de cada filial. Sin embargo, en el caso en que los supervisores del país de acogida de una filial estimen que los requerimientos de capital han de calcularse de manera independiente, dicha filial no podrá incorporar los beneficios de la diversificación a escala del grupo en sus cálculos de AMA (por ejemplo, cuando la filial de un banco internacionalmente activo se considere significativa, la filial podrá incorporar los beneficios de la diversificación de sus propias operaciones, es decir, los que procedan del nivel subconsoldidado, pero no podrá hacerlo de los procedentes del banco matriz).

Método de Medición Avanzada (AMA)

Capital de Riesgo Operacional = a aquel medido y calculado por el sistema de medición de riesgo propio del banco

Una sólida y adecuada administración de riesgo garantiza el equilibrio operativo de las instituciones financieras, lo que permite valorar apropiadamente las operaciones de riesgo, al tiempo que coadyuva a una precisa valoración de los resultados obtenidos en las operaciones, y por ende a reflejar una real retribución a los recursos propios. El objetivo de cada uno de los métodos es que las instituciones financieras (banca) privadas, implemente de acuerdo a sus posibilidades algún método de valorización del riesgo, pero con la obligación de perfeccionar el mismo y llegar a métodos de valorización del riesgo avanzado, es de vital importancia que las instituciones financieras implementen mecanismos y procesos; así como cuenten con recursos humanos calificados y experimentados en el control de los riesgos generados por sus operaciones; todo ello a los fines de que logren identificar, medir, monitorear, limitar, controlar, informar y revelar claramente los diferentes tipos de riesgo a que están expuestas.

La administración integral de riesgos, supone la adecuación de la estructura organizativa de las instituciones financieras, a los fines de establecer la unidad administrativa y operativa requerida para la valoración, control y monitoreo de los niveles de riesgos asumidos. El objetivo final de la SUBEBAN es la autorregulación por parte de las instituciones financieras o los sujetos de aplicación de la resolución 136.03.

Otro aspecto importante en el desarrollo de una robusta infraestructura de seguridad es la mitigación de los delitos informáticos. “La ONU define los delitos informáticos, a cualquier actividad o conductas ilícitas, susceptibles de ser sancionadas por el derecho penal, que en su realización involucre el uso indebido de medios informáticos”[15]. Existen tres tipos de delitos reconocidos por la ONU: Fraude cometido mediante la manipulación de computadoras, daños o modificaciones de programas o datos informáticos, acceso no autorizados a servicios o sistemas informáticos.

1) Fraudes cometidos mediante manipulación de computadoras.

✓ Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos, en la fase de adquisición de los mismos.

✓ La manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado “Caballo de Troya”, consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

✓ Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos, mediante la falsificación de instrucciones para que la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían en bases de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

✓ Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de

[15] Presentación en las III Jornadas de “Delitos Informáticos”- SUSCERTE.

transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otros.

2) Daños o modificaciones de programas o datos computarizados.

✓ Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas más comunes que permiten cometer sabotajes informáticos son:

Virus: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada.

Gusanos: se fabrica de forma análoga al virus, con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse

Bomba lógica o cronológica: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro, ya que se activa según una condición. Ahora bien, al contrario de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño

3) Accesos no autorizados a servicios y sistemas informáticos**.**

✓ El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación: el delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento o que vienen por defecto, que están en el propio sistema.

✓ Reproducción no autorizada de programas informáticos. Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como “delito” esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

A partir del auge de las redes, en este nuevo modelo informático descentralizado y distribuido, con sus nuevos modelos de integración entre clientes, servidores y servicios que a menudo operan en otros dominios, la seguridad comenzó a ser una parte integral y aglutinadora del tejido informático.

Hasta hace un tiempo atrás, muchos creían que el villano de la información era el hacker, una persona de pelo largo, y aspecto tenebroso, oculto tras un computador de última tecnología en un lugar oculto de algún país con nombre desconocido. Sin embargo, esto ha pasado a ser un mito de la informática.

Este error ha sido reafirmado por numerosas estadísticas que demuestran que un porcentaje de los problemas de seguridad se produce en el interior mismo de las organizaciones. Empleados insatisfechos, usuarios curiosos y por sobre todo poco conscientes del impacto que pueden tomar sus acciones en una red, en un sistema.

Algunos datos sobre el delito informático.

"Una encuesta desarrollada por expertos en seguridad y representantes de la publicación CSO magazines en colaboración con el Servicio Secreto de los Estados Unidos y el CERT/CC de la Universidad de Carnegie Mellon sobre el estado de la seguridad y el delito informático" [16], reportaron un incremento de delitos informáticos e intrusiones en sus redes, sistemas o datos, tal como se reseña en los siguientes párrafos:

1) El 43% de los encuestados confirmaron un incremento de las intrusiones y delitos informáticos respecto del año anterior. Incluso, un 70% denunciaron al menos un delito o intrusión contra su organización.

2) El 32% de las victimas de intrusiones y delitos informáticos no siguen la pista de las perdidas por los delitos informáticos o las intrusiones, e incluso, aquellos que si realizan la adecuada investigación, la mitad no conocen la cantidad de pérdida total. Un porcentaje de un 41% indicaron que no poseen un plan formal para comunicar, denunciar y responder ante este tipo de delitos, lo que demuestra que hay cabida para mejorar este tipo de políticas.

3) El 30% de los encuestados que sufrieron delitos e intrusiones, no llegaron nunca a conocer si el atacante era desde dentro de la organización o remoto. Los encuestados que sí conocían dicho dato, confirmaron que en un 71% los ataques venían desde el exterior, comparado con un 29% que fueron realizados por empleados.

[16] Encuesta del Carnrgie Mellon University.

4) Según la compañía anti-virus Trend Micro, los virus y gusanos “online” han obstruido sistemas informáticos y dejado fuera de operación a páginas web vitales, costando cerca de 55.000 millones de dólares en productividad el pasado año.

5) Estudios realizados por el Sans Institute y el FBI señalan que el 90% de los delitos informáticos pueden ser evitados, con una programa de concientización de usuarios, aplicación de fuertes medidas de seguridad, y un monitoreo constante.

6) El 70% de los ataques bajo la modalidad de hackers, son provocados por funcionarios descontentos.

Las organizaciones venezolanas y muy especialmente los bancos privados no son ajenos a este fenómeno que es ocasionado por la utilización de tecnología de información para la ejecución de acciones delictivas, en Venezuela no encontramos estadísticas sobre este tipo de delitos, las unidas referencias son las obtenidas por la clonación de tarjetas de crédito y debito. Es posible que por una combinación de razones económicas y psicológicas, probablemente se denuncie sólo un número muy limitado de delitos informáticos. Dado que atentan contra el mismo concepto de seguridad tecnológica, las empresas pueden muy bien ser reacias a admitir que sus medidas de seguridad no son lo suficientemente robustas.

COMO DISMINUIR EL RIESGO DE SER VICTIMA DE UN DELITO INFORMÁTICO

En la actualidad dependemos cada vez más de las redes electrónicas de comunicación, por lo cual cada vez somos más vulnerables a los ataques. Para prevenir posibles ilícitos informáticos, resulta conveniente incentivar la conciencia de control y seguridad sobre los sistemas y recursos informáticos, para lo cual debemos considerar al menos los siguientes puntos:

1) Implementación de controles que impidan el acceso no autorizado a los servidores y computadoras. En el caso de una compañía, por ejemplo, es conveniente que se restrinja el acceso físico a los servidores e instruir a los usuarios para que no divulguen sus contraseñas.

2) Definición de permisos de accesos según las funciones del personal dentro de la compañía. A cada usuario se le otorgan permisos para poder realizar determinadas tareas, acceder a información sensible de acuerdo a su función dentro la compañía. Por ejemplo, leer pero no modificar archivos o carpetas, utilizar o no la conexión a Internet, etc.

3) Ejecución de un plan de auditorias periódicas. Implementar un sistema de auditoria que permite guardar información relativa a lo que las personas hacen en un sistema informático. Esto permite luego monitorear las operaciones que un usuario ha realizado.

En este nuevo universo de informática integrada en evolución, la seguridad es un aspecto clave. Las organizaciones deben de tener las garantías de que sus sistemas y otros componentes tecnológicos están a salvo de ataques. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados.

Uno de los retos más importantes en la lucha contra el delito informático es estimar su incidencia, su escala y su costo que permita poder definir los tipos de medidas a adoptar y garantizar su proporcionalidad. En este sentido, leyes como Sarbanes-Oxley- EEUU define a "los ejecutivos como responsables de la seguridad informática al requerir que den su palabra de que los "controles internos" de las compañías son ad[17]ecuados".

En Venezuela, hay un marco legal sobre los delitos informáticos y el uso de la tecnología de información de reciente promulgación y aplicación. Las regulaciones más importantes las encontramos en las siguientes leyes:

Ley Especial sobre Delitos Informáticos: "Tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en dicha ley"[18]. Esta ley tipifica los delitos y establece penas con sus circunstancias agravantes y atenuantes y también penas accesorias, entre las clases de delitos que establece se encuentran:

- ✓ Contra los sistemas que utilizan tecnologías de información.
- ✓ Contra la propiedad.
- ✓ Contra la privacidad de las personas y de las comunicaciones.
- ✓ Contra niño y adolescente.
- ✓ Contra el orden económico.

[17] Ley Sarbanes-Oxley,Deloitte
[18] Ley Especial sobre los Delitos Informáticos, Republica Bolivariana de Venezuela.

1) Los delitos contra los sistemas que utilizan tecnología de información son los siguientes:

✓ El acceso indebido a un sistema, penado con prisión de uno a cinco años y multa de 10 a 50 unidades tributarias (UT).

✓ El sabotaje o daño a sistemas, incluyendo cualquier acto que altere su funcionamiento, penado con prisión de cuatro a ocho años y multa de 400 a 800 UT, que aumentará a prisión de cinco a diez años y multa de 500 a 1.000 UT si para su comisión se utiliza un virus o medio análogo. Si se trata de sabotaje o daño culposo, la pena se reduce entre la mitad y dos tercios. Si se trata de sabotaje o acceso indebido a sistemas protegidos, la pena aumenta entre la tercera parte y la mitad.

✓ La posesión de equipos o prestación de servicios para actividades de sabotaje, penado con prisión de tres a seis años y multa de 300 a 600 UT.

✓ El espionaje informático, que incluye la obtención, difusión y revelación de información, hechos o conceptos contenidos en un sistema, penado con prisión de tres a seis años y multa de 300 a 600 UT. Si el delito se comete para procurar un beneficio para sí o para otro, la pena aumenta entre un tercio y la mitad. El aumento será de la mitad a dos tercios si se pone en peligro la seguridad del Estado, la confiabilidad de la operación de las personas afectadas o si como resultado de la revelación alguna persona sufre un daño.

✓ La falsificación de documentos mediante el uso de tecnologías de información, o la creación, modificación o alteración de datos en un documento, penado con prisión de tres a seis años y multa de 300 a 600 UT. Si el delito se comete para procurar un beneficio para sí o para otro, la pena aumenta entre un tercio y la mitad. Si el hecho resulta en un perjuicio para otro, el aumento será de la mitad a dos tercios.

2) Delitos contra la propiedad: La técnica legislativa utilizada en este caso es incorrecta, pues a delitos ya previstos en la codificación penal se les crea una supuesta independencia, cuando la única diferencia existente es el medio utilizado (electrónico en lugar de mecánico o material) y la naturaleza del bien tutelado, que en este caso es intangible, mientras que en los bienes muebles es física. En esta clase se incluyen:

✓ El hurto, que consiste básicamente en apoderarse de un bien o valor tangible o intangible de carácter patrimonial, sustrayéndolo a su tenedor mediante el acceso, interceptación, interferencia, manipulación o uso de un sistema que utilice tecnologías de información, penado con prisión de dos a seis años y multa de 200 a 600 UT.

✓ El fraude realizado mediante el uso indebido de tecnologías de información, penado con prisión de tres a siete años y multa de 300 a 700 UT.

✓ La obtención indebida de bienes o servicios mediante el uso de tarjetas inteligentes (tarjetas de crédito, de débito o de identificación que garanticen el acceso a un sistema reservado u otras similares, penado con prisión de dos a seis años y multa de 200 a 600 UT.

✓ El manejo fraudulento de tarjetas inteligentes, o la creación, duplicación o incorporación indebida de datos a registros, listas de consumo o similares, penado con prisión de cinco a diez años y multa de 500 a 1.000 UT. La misma pena será impuesta a quienes sin tomar parte en los hechos descritos se beneficien de resultados obtenidos.

✓ La apropiación indebida de tarjetas inteligentes, penado con prisión de uno a cinco años y multa de 10 a 50 UT. La misma pena se impondrá a quien reciba o adquiera dichas tarjetas.

✓ Provisión indebida de bienes o servicios utilizando una tarjeta inteligente, a sabiendas de que dicho instrumento ha sido falsificado, está vencido o ha sido alterado, penado con prisión de dos a seis años y multa de 200 a 600 UT.

✓ La posesión de equipos para falsificaciones, penado con prisión de tres a seis años y multa de 300 a 600 UT.

3) Los delitos contra la privacidad de las personas y las comunicaciones son los siguientes:

✓ La violación de la privacidad de la data o información de carácter personal que se encuentre en un sistema que use tecnologías de información, penado con prisión de dos a seis años y multa de 200 a 600 UT. Esta pena se aumentara de un tercio a la mitad si como consecuencia del delito descrito resulta un perjuicio para el titular de la información o para un tercero.

✓ La violación de la privacidad de las comunicaciones, penado con prisión de dos a seis años de prisión y una multa de 200 a 600 UT. El tema de la privacidad ha sido uno de los más discutidos en los ordenamientos jurídicos extranjeros, debido a los derechos humanos. Las discusiones se han concentrado, básicamente, en la posibilidad de que el empleador revise las conversaciones y envío de datos de los empleados que utilizan como medio el sistema del empleador, así como la propiedad de la información contenida en del sistema del empleador” [19].

[19] Las fronteras de la ley ,CAVECOM-E, 1999

✓ La revelación indebida de datos o información obtenidos por los medios descritos en los literales anteriores, penado con prisión de dos a seis años y multa de 200 a 600 UT. Esta pena se aumentara de un tercio a la mitad si el delito se cometió con fines de lucro o si resulta en un perjuicio para otro. Con relación al tema se ha centrado en la posibilidad de que el dueño de un sistema venda información personal de los usuarios del sistema con fines de comercialización.

4) Los delitos contra niños y adolescentes son los siguientes:

✓ La difusión o exhibición de material pornográfico sin la debida advertencia para que se restrinja el acceso a menores de edad, penado con prisión de dos a seis años y multa de 200 a 600 UT.

✓ La exhibición pornográfica de niños o adolescentes, penado con prisión de cuatro a ocho años y multa de 400 a 800 UT.

5) El último tipo contempla los delitos contra el orden económico, que son los siguientes:

✓ La apropiación indebida de propiedad intelectual mediante la reproducción, divulgación, modificación o copia de un software, penado con prisión de uno a cinco años y multa de 100 a 500 UT.

✓ La oferta engañosa de bienes o servicios mediante la utilización de tecnologías de la información, penado con prisión de uno a cinco años y multa de 100 a 500 UT, sin perjuicio de la comisión de un delito más grave.

Además de las penas principales indicadas anteriormente, se impondrán, sin perjuicio de las establecidas en el Código Penal, las siguientes penas accesorias:

El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la Ley (posesión de equipos o prestación de servicios de sabotaje y posesión de equipos para falsificaciones).

Trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos los artículos 6 y 8 de la Ley (acceso indebido y favorecimiento culposo del sabotaje o daño).

La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del

ejercicio de un cargo o función pública, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada.

La suspensión del permiso, registro o autorización para operar o para ejercer cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se valió de o hizo figurar a una persona jurídica.

Además, el tribunal podrá disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Ley sobre Mensajes de Datos y Firmas Electrónicas: "Tiene por objeto reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y a los Certificados Electrónicos"[20].

Homologa los efectos de la firma autógrafa a la firma electrónica. Establece los requisitos mínimos que confieran seguridad e integridad a los mensajes de datos y a la firma electrónica; establece los requisitos mínimos que debe tener un Certificado Electrónico; crea un Registro de Proveedores de Servicios de Certificación; crea la Superintendencia de Servicios de Certificación Electrónica para registrar y supervisar a los Proveedores de Servicios de Certificación.

Con estos elementos principales y otros que se establecen en este proyecto de ley, se brinda seguridad y certeza jurídica a los actos y negocios electrónicos, mientras se perfeccionan y estandarizan los usos, costumbres y modos de relacionarse y comerciar por este medio a nivel mundial.

En conclusión, las leyes llenan parcialmente un vacío legislativo en una materia de mucha importancia, sin embargo, múltiples deficiencias y problemas en la técnica legislativa empleada y los conceptos usados, así como diversas lagunas y contradicciones, la hacen insuficiente como complemento del resto de la legislación.

Las organizaciones y sus empleados deben apegarse al conjunto de normas y leyes dispuestas por el Estado, la industria y el entorno.

---

[20] Ley sobre Mensajes de Datos y Firmas Electrónicas, Republica Bolivariana de Venezuela 2001.

CAPITULO III
MARCO METODOLÓGICO

Tipo de Investigación

El tipo de investigación se identifica como proyecto factible. Los estudios factibles sirven para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes, así como, las posibles soluciones a los mismos. También, como definir las condiciones en que se presenta y las distintas maneras en que puede manifestarse.

Los proyectos factibles detallan con mayor precisión la singularidad de una realidad estudiada, como por ejemplo, las medidas de seguridad en un ambiente computacional.

Diseño del Proyecto

Con relación al marco del proyecto planteado, referido al establecimiento de un sistema de seguridad para las instituciones financieras privadas en Venezuela, el diseño se orientó desde un punto de vista técnico y documentar sobre las principales brechas de seguridad publicadas por las principales instituciones (Cobit, ISO17999, BS 7799, ITIL, Mejores Prácticas, Microsoft).

Este trabajo se orientó dentro de una combinación de investigaciones documentales, de sistematización de las mejores prácticas, tomando de cada una de ella la solución técnica más adecuada a la brecha de seguridad analizada. La idea no es realizar un estudio del mercado sobre las recomendaciones, sino tomar, lo mejor de cada una de ellas, por ejemplo, las recomendaciones de Microsoft, son aplicadas a los productos o servicios que ellos distribuyen. Si aplicamos alguna recomendación sobre una tecnología de la cual ellos nos son propietarios, es casi seguro que el resultado no será el deseado. Si bien las normas o mejores prácticas de debido cuidado, son ampliamente aceptadas y apoyadas, desafortunadamente no existe en la actualidad una norma mundial que defina las políticas específicas de seguridad informática.

Este trabajo esta dividido en etapas, la primera, consiste en el estudio de las principales amenazas (internas o externas) conocidas hasta el momento que puede ser susceptible las instituciones financieras privadas del país (bancos) , este trabajo cuenta con el apoyo de bibliografía básica, trabajos previos, información y datos divulgados por medios impresos e Internet.

La segunda etapa, es la búsqueda de la mejor práctica aplicable a la brecha o amenaza de seguridad reportada. La contramedida indicada procede de alguno de los estándares aplicado por la industria.

Es importante tener presente que las normas técnicas, ISO 17799, BS 7799, ITIL y Las Mejores Prácticas, son neutrales en cuanto a la tecnología. Así por ejemplo, la norma discute la necesidad de contar con firewalls, pero no profundiza sobre los tipos de firewalls y cómo se utilizan.

Todos estamos conscientes del reto que significa el acceso a grandes masas de información, el cual es permitido por los sistemas de información computarizados con el fin de manipularla, modificarla y destruirla. Los cambios producidos por la tecnología de información sobre los procesos de generación y transmisión de datos son dramáticos, aun en las sociedades menos desarrolladas.

Vemos como pasamos de una sociedad altamente centralizada, dependiente, agraria; a una altamente industrializada con alta tecnología. Así, podemos decir que el progreso del hombre va totalmente relacionado con la ética y comportamiento del mismo. En este sentido, la tecnología es creada por los humanos y depende de ellos su uso y "abuso".

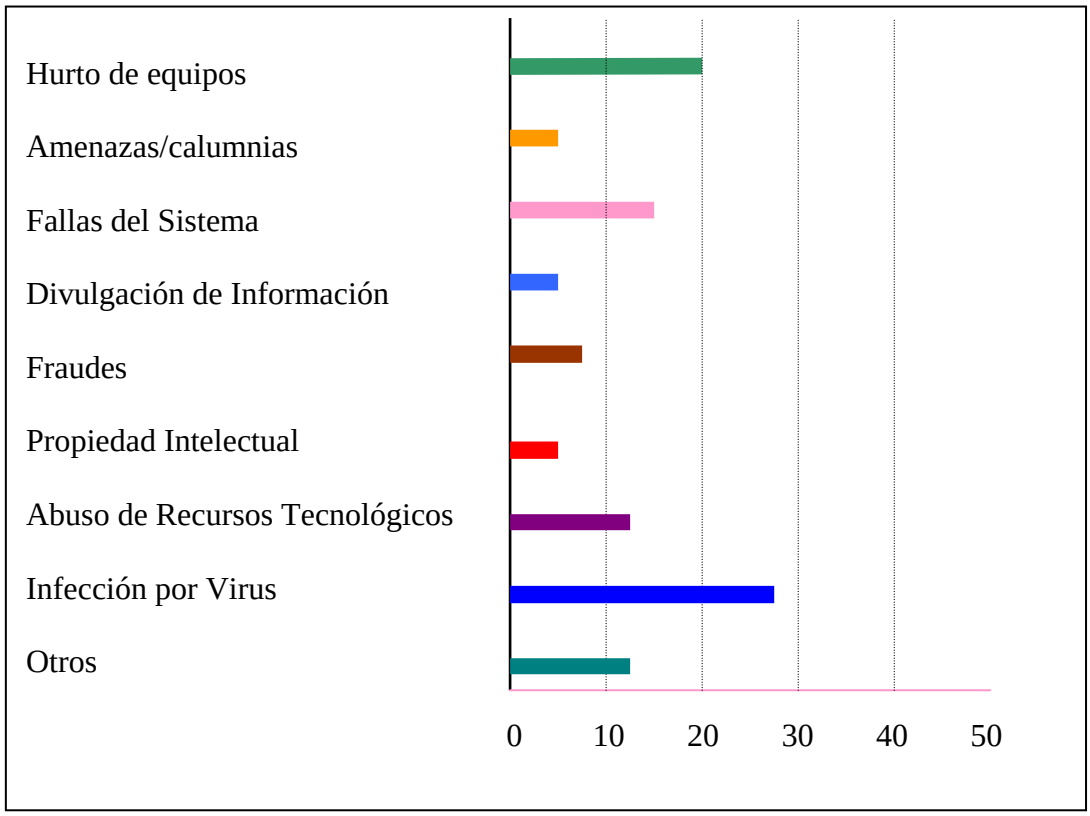
La idea que el ser humano pueda discernir desde la adolescencia, no es completamente aplicable cuando estamos hablando de una persona que utiliza un computador. En otras palabras, la tecnología de información es relativamente tan reciente que las sociedades, los maestros y la gente muchas veces tienen poca experiencia en el manejo de la misma, y a veces no se imaginan su potencialidad, retos y riesgos. Muchos de los usuarios finales de computadores no conocen las consecuencias del uso, abuso, y de sus acciones sobre el colectivo en un sistema de información computarizado. Por tanto, muchos de ellos estarán a la deriva dependiendo de su juicio y de lo que ellos crean como sentido común. Por ejemplo, es normal oír de parte de potenciales o reales "hackers" algo como esto: "Si ellos no quisieran que la gente penetrara a sus sistemas, habrían utilizado mejores medidas y mecanismos de seguridad".

Definido así el proyecto, se realizó un inventario de las principales fuentes o posibles focos de amenazas sobre un ambiente computacional de una organización bancaria privada en Venezuela.

Recientemente la firma Espiñeira, Sheldon y Asociados miembro PricewaterhouseCoopers, publicó en febrero del 2006, un trabajo "sobre las brechas de

seguridad y controles de seguridad en las empresas venezolanas (pc-news_com)[21]". En el gráfico 1 se observar los principales incidentes de seguridad reportados.

Gráfico N° 1. Incidentes de seguridad de activos de información reportados en el último año



En cada área de posible amenaza, se indicarán las mismas y cuales pueden ser las contramedidas para la solución de las brechas de seguridad planteadas.

Es importante tener presente que las brechas de seguridad y las contramedidas aquí planteadas son las conocidas al momento de la elaboración del presente trabajo, posiblemente aparezcan nuevas amenazas sobre la seguridad de la información.

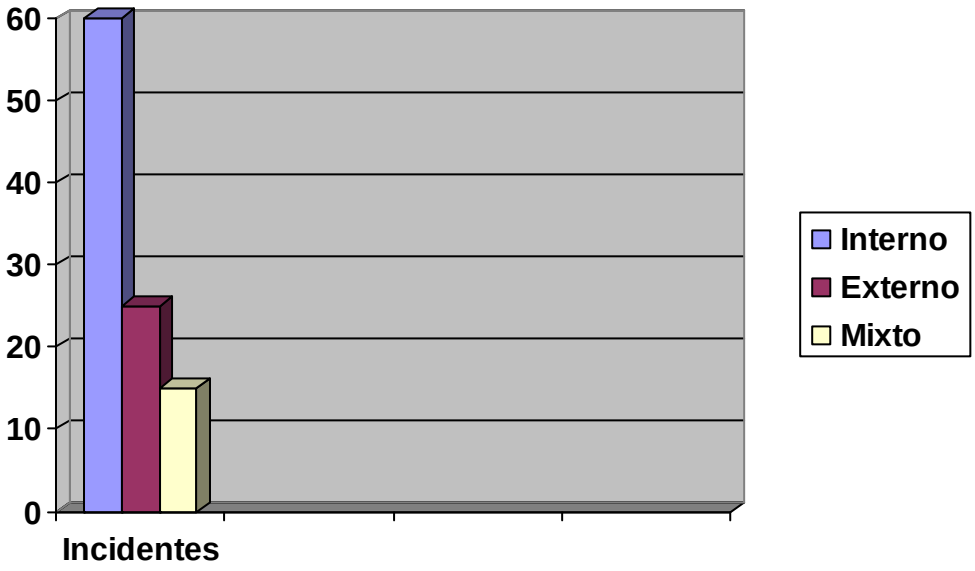
Las instituciones financieras siempre han estado expuestas a riesgos de seguridad de activos de información, tales como divulgación indebida de la información, fraudes, fallas de hardware o software, planificación no efectiva de actividades y riesgos asociados con las operaciones de usuarios finales; pero el impacto de estos riesgos y la velocidad con la cual surgen, han cambiado dramáticamente, requiriendo hoy en día una respuesta inmediata y efectiva de control.

[21] www. Revista PC-News.com

Sin embargo, y para analizar los riesgos del sector bancario con una visión más amplia, es importante mencionar, que la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN), considera las siguientes categorías de riesgos: riesgo de liquidez, riesgo operacional, riesgo de mercado, riesgo de interés, riesgo cambiario, riesgo de precio, riesgo legal, riesgo reputacional.

Dentro del riesgo operacional ubicamos el riesgo tecnológico, el cual tiene dos vertientes: las amenazas internas, las externas y una combinación de ambas, el gráfico 2 indica el origen del los principales incidentes de seguridad.

Gráfico 2, origen del peor incidente de seguridad de activos de información reportado en las organizaciones en el año 2004



Comenzaremos por definir que son riesgos o vulnerabilidades, “Una vulnerabilidad es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil”[22].

[22] www. Guía de operaciones de seguridad para Windows 2000 Server

CAPITULO IV

PROPUESTA y RECOMENDACIONES

Medidas Internas

La primera medida que implementamos para el establecimiento de un modelo de seguridad, es la creación y publicación del Manual de Seguridad de Activos de Información o Manual de Seguridad, las políticas de seguridad conforman el conjunto de lineamientos que debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Las políticas de seguridad de activos de información constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad.

Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general. Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización.

Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización.

Este manual fue realizado tomando las “mejores practicas internacionales”[23] , con dicho Manual cumplimos con uno de los objetivos específicos “Documentar y Proponer una serie de políticas y normas orientadas a la protección de Activos de Información”. Ver anexo 1.

Otro de los objetivos de nuestro trabajo es “proponer la estructura y ubicación de la gerencia de seguridad de datos dentro de las organizaciones” , para este fin debemos tener presente una de las recomendaciones de las “mejores práctica internacional” y a la cual se han acogido las empresas de Auditoria Externas y SUDEBAN, la misma establece que dicho departamento no debe de tener una línea de reporte subordinada al área de tecnología, bajo esta premisa algunas organizaciones financieras han tomado la decisión de que el departamento de seguridad de datos reporte a la gerencia general de

[23] Políticas De Seguridad Informática, ”Mejores Practicas Internacionales”,

operaciones y tecnología, desde nuestro punto de vista esta ubicación no es la más adecuada ya que debemos de tener presente que esta unidad requiere de un nivel de independencia y objetividad similar a la de Auditoria y no debería reportar a la misma gerencia a la cual esta subordinada el área de tecnología, nuestra propuesta es que dicha unidad reporté a un área de control con suficiente independencia. Ver figuras 6 y 7, donde se esbozan “posible ubicación del Departamento de Seguridad de Datos”.

Figura 6
Propuesta 1
Ubicación de Seguridad de Datos

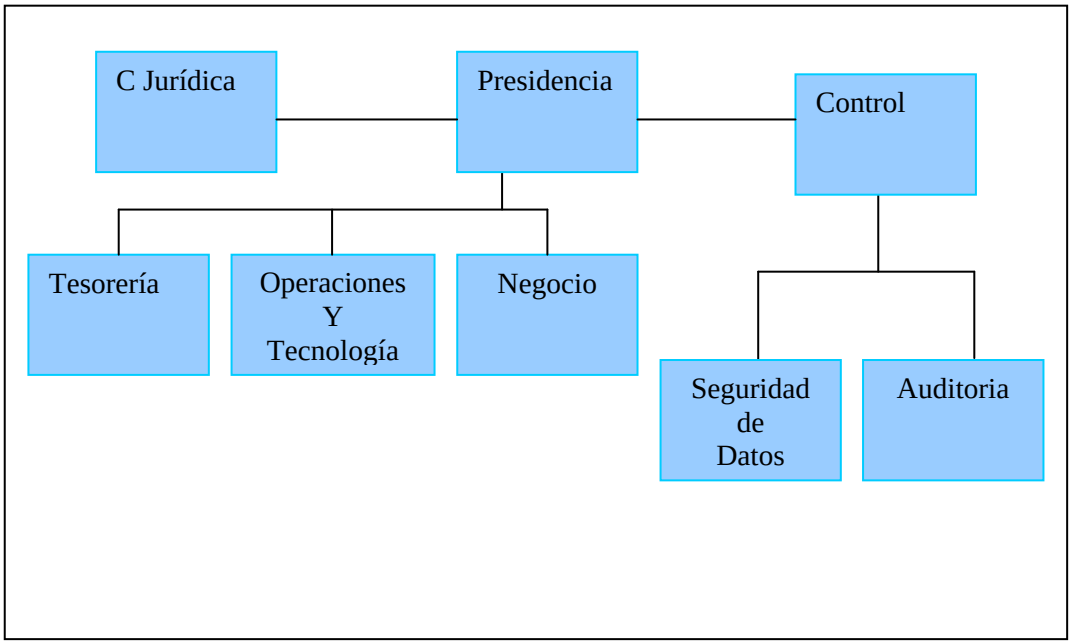
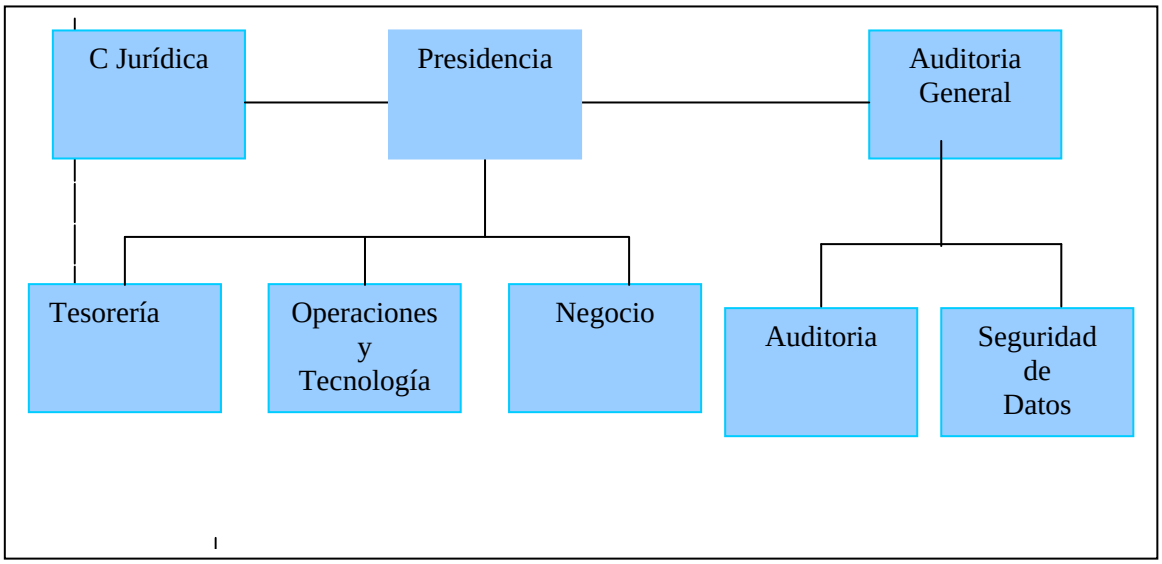


Figura 7
Propuesta 2
Ubicación de Seguridad de Datos



Otro aspecto importante, es la cantidad de empleados y el conocimiento que los mismos debe de poseer sobre el tema de seguridad de datos, dado el grado de sensibilidad del área, es recomendable que los empleados tengan conocimientos específicos sobre las funciones para las cuales están asignados. Dependiendo del tamaño de la organización y de las herramientas tecnológicas destinadas al área de seguridad de datos, él numero de empleados será de 4 a 8 personas, las cuales recomendamos sea distribuidas: a) para la creación de acceso y desbloqueo de claves 1, b) monitoreo de la red interna 1, c) monitoreo de la red externa 1, d) control de cambio 1.

Dentro del alcance de este trabajo se encuentra “documentar cuales mecanismos de seguridad son apropiados para la protección de la información de las amenazas internas”

Las amenazas que provienen del interior de la organización pueden ser especialmente costosas porque el infractor tiene mayor acceso y conocimiento sobre el lugar donde reside la información importante y confidencial.

Las amenazas internas pueden ser actos deliberados de sabotaje, iniciado por un empleado descontento o un error inocente cometido por un trabajador bien intencionado que tiene un nivel inadecuado de acceso al sistema crítico, el impacto producido por la

información comprometida, robada, dañada o borrada puede ser de grandes proporciones.

Contramedidas

Se incluyeron dentro del manual de seguridad de activos de información varias políticas para definir los recursos valiosos de información de la compañía y todos los derechos de acceso a esa información. Las mismas fueron publicadas para que todos los usuarios conozcan las políticas.

Es importante que los empleados conozcan los riesgos de permitir que otras personas tengan acceso a sus cuentas y contraseñas. Adicionalmente, es necesario alértelos sobre los peligros de la “ingeniería social” por medio de la cual los intrusos buscan obtener acceso no autorizado a la información al aprovecharse de la ingenuidad de los usuarios. Quizás el mejor ejemplo de ingeniería social son los correos electrónicos que parecer provenir de un amigo y están acompañados de un archivo adjunto ejecutable que contiene un virus. La ingeniería social aprovecha el deseo humano de “hacer lo correcto”, por lo cual usted debe crear consciencia en los usuarios sobre este tipo de ataques.

Es recomendable que los empleados tengan acceso únicamente a la información y a los sistemas que necesitan. Esto puede sonar elemental, pero no es raro que los empleados tengan de 10 a 20 veces más acceso a los recursos de lo necesario para realizar su trabajo.

Si cree que es necesario, puede restringir el acceso mediante la implementación de software especializado de control al acceso. Este software se puede utilizar para limitar las actividades del usuario relacionadas con sistemas o archivos específicos y llevar los registros de las actividades individuales de los usuarios en la computadora.

Si las "relaciones de confianza" con contratistas externos les exigen tener acceso a la red, asegúrese de que el acceso sea asignado únicamente para los servicios específicos requeridos. Es común que los usuarios necesiten acceso a la información de diferentes niveles de valor. Cuando asigne los niveles de acceso, asegúrese de que un nivel de protección no exponga a más de un recurso valioso.

Recomendamos suministrar a los contratistas y trabajadores temporales cuentas de red que tengan "fechas de terminación" automáticas después de las cuales dejan de funcionar a menos que sean prolongadas.

Nunca es fácil mencionar el tema de las amenazas de intrusos internos. En un mundo ideal, confiaríamos incondicionalmente en todos nuestros empleados. Sin

embargo, la realidad es que trabajamos en un entorno imperfecto donde las amenazas pueden surgir desde el interior de las cuatro paredes. Aunque las políticas y procedimientos son esenciales para confrontar este problema, se necesitan diligencia y determinación para resolverlo.

Las Contraseñas

Las contraseñas son la primera línea de defensa contra el acceso desautorizado a los sistemas de información son las llaves para entrar a cualquier sistema, por lo que es una medida de seguridad para restringir los accesos a los sistemas de computación y sus recursos. Todos los credenciales de acceso son de uso personal, y no pueden ser almacenados, anotados o revelados a otro individuo, las mismas deben ser de difícil deducción o calculo.

Contramedidas

Una contraseña es un conjunto de caracteres que deben proporcionarse antes de un inicio de sesión o que un acceso sea autorizado. Una contraseña puede componerse de letras, números, símbolos, y la misma puede ser sensible a minúsculas y mayúsculas.

Una contraseña robusta debe por lo memos tener (8) caracteres ,no contener todo o parte del nombre de su cuenta de usuario, y contemplar tres de las cuatro categorías siguientes de caracteres:

1) Letras mayúsculas (A, B, C ....)
2) Letras minúsculas (a, b, c,....)
3) Los números (0,1,2,3,4.....)
4) Los símbolos encontrados en el teclado (-, ¡, %; @., {, $....)

Adicionalmente una contraseña robusta debe:

1) No contener su nombre de usuario, nombre real, nombre de la compañía, o del mes en curso.
2) No contener una palabra completa del diccionario.
3) Ser significativamente diferente de las contraseñas anteriores.

Un ejemplo de una contraseña robusta es Bu2nos_Di3as.

Amenazas de los Virus

Los virus informáticos son programas diseñados expresamente para interferir en el funcionamiento de una computadora, registrar, dañar o eliminar datos, o bien para propagarse a otras computadoras y por Internet, a menudo con el propósito de hacer más lentas las operaciones y provocar otros problemas en los procesos.

Para su propagación, los virus básicos suelen requerir que los usuarios desprevenidos los compartan o los envíen inadvertidamente. Algunos virus más sofisticados, como los gusanos, pueden reproducirse y enviarse automáticamente a otras computadoras cuando consiguen controlar determinados programas, como algunas aplicaciones de correo electrónico compartido. Ciertos virus, denominados troyanos (en referencia al legendario caballo de Troya), pueden presentarse como programas aparentemente beneficiosos para que los usuarios los descarguen. Existen incluso algunos troyanos que pueden ofrecer los resultados esperados y, al mismo tiempo, dañar discretamente el sistema local o el de otras computadoras conectadas a la red.

Mito: Los incidentes de infección por virus son un problema meramente técnico.

Realidad: El marco integral de seguridad de los activos de información posee un alto grado del componente relacionado con la educación del personal.

Contramedidas

No hay nada que pueda garantizar al 100% la seguridad de las computadoras y servidores. Sin embargo, se puede seguir mejorando la seguridad de los equipos y reducir las posibilidades de infección si mantiene el sistema actualizado y una suscripción a software antivirus, además de seguir ciertas prácticas recomendadas.

Dado que no hay ningún método de seguridad garantizado, es importante realizar periódicamente copias de seguridad de los archivos importantes, en previsión de virus u otros problemas.

Es necesario la suscripción a un software antivirus estándar y mantenerlo actualizado.

No abra nunca un archivo adjunto a un mensaje de correo electrónico si no conoce al remitente.

No abra archivos adjuntos a mensajes de correo electrónico de remitentes conocidos si desconoce la naturaleza del archivo. El remitente podría no saber que contiene un virus.

Dispositivos de almacenamiento externos.

La tecnología en su avance constante ha hecho, de un tiempo a esta parte, que la multiplicación de dispositivos portátiles de almacenamiento haya crecido considerablemente. Dicho crecimiento se refleja en la funcionalidad que le da al usuario común y corriente, como al corporativo.

Los dispositivos portátiles de almacenamiento están teniendo uso en muchas aplicaciones de la informática personal: reproductores de música, cámaras digitales, reproductoras de vídeo, e incluso, teléfonos celulares. Todos ellos utilizan tecnologías similares (discos flash) con distintos nombres: Compact Flash (CF), Unidades Flash, Memory Stick, Microdrives, Mini Card, Multi Media Card (MMC), Secure Digital (SD), Smartmedia, y XD-Picture Card.

Por otro lado, la introducción de buses universales para la conexión de dispositivos portátiles como son el estándar Universal Serial Bus (USB) y el Estándar Firewire (IEEE 1394) en los computadores ha llevado a la propagación de dispositivos que utilizan estas interfaces, entre ellos, de nuevo, dispositivos de almacenamiento.

Debido a la limitación de capacidad de los basados en tecnología flash, han proliferado en el mercado de consumo los denominados “discos duros externos”, que no son sino discos duros de consumo y tamaño reducido que ofrecen una capacidad de almacenamiento muy superior a los compactos. En la actualidad es posible encontrar, a precios razonables, discos duros USB de 500 GB y Firewire de 1.000 GB.

Ello demuestra que el aumento de dichos dispositivos y las economías de escala logran una disminución constante de precio, al mismo tiempo que aumenta la capacidad de estos dispositivos.

Existen muchos riesgos asociados a este tipo de dispositivos, debido a la capacidad de almacenamiento que poseen y a su tamaño, aspectos que facilitan al intruso o al empleado interno cualquier acción en contra de la información. A continuación señalaremos algunos riesgos, como para hacernos a una idea global de contra que nos enfrentamos. Entre las múltiples cosas que se pueden hacer están las siguientes:

1) Extraer información de la empresa y transportarla fuera de ésta.
2) Introducir programas no autorizados desde el exterior (potencialmente maliciosos), en algunos casos, con ejecución de código automático sin intervención del usuario.
3) Comprometer el equipo a través del arranque de un dispositivo desde la BIOS.
4) “Atacar” al sistema operativo a través de controladores de dispositivos maliciosos o mal programados

Los tres primeros riesgos no son desconocidos; indiscutiblemente, ya existían incorporados a cualquier dispositivo de almacenamiento externo como lo son los diskettes o CD, por nombrar los más conocidos. Lo que sucede es que el nivel de riesgo

de estos dispositivos es mucho mayor toda vez que no es comparable en ningún orden la cantidad de información que pude guardar un CD o un diskette a la que puede transportar un disco portátil. La diferencia es de gran tamaño, pues si realizamos una comparación de un disco portátil y un DVD-Rom notaremos que hoy en día una persona puede transportar el equivalente a 60 DVD en un dispositivo que fácilmente puede ser llevado en la mano o en el bolsillo de su pantalón.

Cuando en una organización el uso de estos dispositivos esta permitido se convierte en cultura, lo que hace difícil controlar los riesgos y poner limites a su utilización, control que no obstante es de vital importancia si se pretende evitar fugas de información.

Contramedidas

Se inició una labor de toma de conciencia por parte de los usuarios sobre los riesgos incorporados a estos dispositivos y controlar el puesto de trabajo para impedir su mal manejo.

Deshabilitar la carga de dispositivos USB, bien modificando el registro o bien eliminando el controlador del sistema para que éste no pueda cargarse.

Modificar la lista de dispositivos “reconocidos” como dispositivos de almacenamiento masivo modificando la lista definida en usbstor.inf, para que sólo un conjunto de dispositivos autorizados puedan hacer que se cargue de forma automática el controlador usbstor.sys.

Deshabilitar la carga de controladores desde Internet.

Bloquear el acceso de escritura a dispositivos de almacenamiento modificando la clave del registro. Esta alternativa sólo es posible en sistemas Windows XP SP2 (KB-555443).

En el caso de sistemas Linux es más sencillo ya que es posible:

Deshabilitar el servicio hotplug para desactivar la carga automática de dispositivos (en Windows no se puede parar el servicio Plug and Play sin inhabilitar gran parte del sistema).

Modificar la configuración del servicio para que no monte automáticamente dispositivos de almacenamiento.

Modificar la configuración de los permisos de montaje para usuarios impidiendo el montaje de dispositivos en el sistema de ficheros o limitando las operaciones que se pueden hacer con éstos (solo lectura, sin permisos de ejecución, etc.).

Existen en el mercado distintas alternativas para su mitigación, que van desde software especifico para el bloqueo de los puertos USB, hasta la aplicación de derechos y permisos por políticas de seguridad, pero por supuesto es importante estar atento a la cantidad de vías de escape de información que esto abre.

Los dispositivos portátiles establecen un riesgo no vigilado hoy en día en la mayoría de las organizaciones, a pesar de disponer de herramientas, tanto en los propios sistemas operativos como las aplicaciones de terceros para restringir y auditar su utilización, y comprimir, por tanto su riesgo.

Correo Electrónico

El correo electrónico se ha convertido en una herramienta fundamental que ha permitido modernizar y agilizar la comunicación y los procesos de la organización con sus múltiplas y conocidas ventajas tales como rapidez y confiabilidad.

La utilización incorrecta de esta herramienta puede ocasionar efectos adversos. Para prevenir esta situación, existen algunos lineamientos de ética y buen uso del correo que contribuyen que la comunicación llegue al destinatario(s) correcto(s), haciendo un mejor uso de los recursos tecnológicos disponibles y más importante aún, del tiempo de todos los participantes de la comunicación electrónica.

Contramedidas

El uso del correo electrónico corporativo debe responder a las necesidades propias del negocio. No es correcta su utilización con fines ajenos a la institución. Su uso con fines personales podrá ser eventual siempre y cuando no exponga a la institución y no interfiera con el rendimiento del personal.

No reenvíe cadenas, alertas de virus, material pornográfico, videos o fotos. En la mayoría de los casos, los correos con alertas son falsas y con intenciones maliciosas (propagación de virus, captura de direcciones de correo válidas que posteriormente son utilizadas para envíos de SPAM)

No responda mensajes que Ud. No haya solicitado o del que desconozca su procedencia. Haga caso omiso a las notas que le hacen petición para desincorporarse de las listas de distribución a través de la cual llegó el correo como REMOVE o UNSUSCRIBE, ya que con ello estará confirmando que su dirección de correo es valida y esta activa.

No suministre su cuenta de correo corporativa en sitios Web no seguros y no relacionados al negocio, así como tampoco en Newsletters, noticias cortas, foros, encuestas, cupones, sorteos, etc.

En el mercado hay una gama de productos que ayudan a una buena administración de esta herramienta de trabajo. El cumplimiento de estas recomendaciones repercutirá positivamente en una mejor administración del sistema de correos, en la optimización de las capacidades de almacenamiento de los buzones, en el uso adecuado de los elementos de comunicaciones (ancho de banda).

Dispositivos de Comunicación

Uno de los elementos de tecnología más importante dentro de una organización que utilice sistema de información para el desarrollo de sus actividades, son las comunicaciones o telecomunicaciones, en las organizaciones financieras el elemento de comunicación lo encontramos desde las estaciones de trabajos (locales o remotas) hasta el los Cajeros Automáticos.

Vulnerabilidades, amenazas y riesgos

Suele ocurrir que ante el imperativo deseo de poner en marcha la solución IT más ventajosa o de querer determinar cuál de las últimas aplicaciones, servidores y bases de datos que mejor se acomodan mejor a los objetivos de una organización, se deje en un segundo plano la protección de la información que contienen todos estos elementos. Es probable que se piense erróneamente que al no haber sido aún víctimas de algún intento de ataque, no existe ninguna amenaza para ellos. Una vulnerabilidad de seguridad es un defecto o debilidad en el diseño, implementación o funcionamiento de un sistema que podría ser utilizado para violar su seguridad. Una vulnerabilidad de seguridad no es un riesgo, amenaza o ataque.

Hay cuatro tipos de vulnerabilidades: vulnerabilidad modelo de amenaza, que resulta de la dificultad para prever amenazas futuras; vulnerabilidad diseño y especificación, producida de errores o descuidos en el diseño del protocolo que lo hacen inherentemente vulnerable (por ejemplo la norma WEP 802.11b del IEEE, también conocida como WiFi); vulnerabilidad implementación, que se produce como resultado de errores en la implementación del protocolo; y para terminar, vulnerabilidad funcionamiento y configuración, que resulta de la utilización errónea de opciones en las implementaciones o de políticas insuficientes de instalación (por ejemplo, cuando el administrador de red no facilita la utilización de la criptación en una red WiFi, o cuando escoge un cifrado de trenes que no es suficientemente robusto).

Conforme a la Rec. UIT-T X.800, una amenaza de seguridad es una violación potencial de la seguridad, que puede ser activa, es decir que existe la posibilidad de un cambio deliberado y no autorizado del estado del sistema, o pasiva, cuando hay

amenaza de revelación no autorizada de la información sin que se modifique el estado del sistema. Ejemplos de amenazas activas son la usurpación de identidad, como entidad autorizada, y la negación de servicio. Un ejemplo de amenaza pasiva es la escucha clandestina tendiente a robar contraseñas no criptadas. Estas amenazas pueden provenir de piratas informáticos, terroristas, vándalos, del crimen organizado, o pueden tener origen en alguna entidad estatal, pero en muchas ocasiones provienen del interior mismo de la organización.

Un riesgo de seguridad ocurre cuando se combinan una vulnerabilidad y una amenaza de seguridad. Por ejemplo, un problema de programación que origine desbordamiento en una aplicación de sistema operativo (es decir una vulnerabilidad) que se asocie con el conocimiento de un pirata, y las herramientas y acceso correspondientes (es decir, una amenaza) puede degenerar en un riesgo de ataque al servidor Internet. Las consecuencias de los riesgos de seguridad son las pérdidas, y corrupción de datos, la pérdida de privacidad, el fraude, el tiempo fuera de servicio, y la disminución de la confianza del público.

Contramedidas

Tomaremos las recomendaciones de, la "X.805 del UIT-T, "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo""[24], la cual define una arquitectura de seguridad de red para proveer seguridad de red de extremo a extremo. Esta arquitectura puede ser aplicada a varios tipos de redes en las que la seguridad de extremo a extremo es una preocupación y es independiente de la tecnología subyacente de la red. Esta recomendación define los elementos arquitectónicos generales relacionados con la seguridad que son necesarios para proveer seguridad de extremo a extremo. El objetivo de esta recomendación es servir como base para desarrollar recomendaciones detalladas para seguridad de red de extremo a extremo.

Esta arquitectura de seguridad fue creada para abordar los retos de seguridad globales de proveedores de servicios, empresas y consumidores y es aplicable a redes inalámbricas, ópticas y alámbricos de voz, información y convergentes. La arquitectura aborda preocupaciones de seguridad para la administración, control y uso de la infraestructura, servicios y aplicaciones de la red. Provee una perspectiva exhaustiva, descendente, de extremo a extremo, de seguridad de red y puede ser aplicada a

[24] Arquitectura de Seguridad para Sistemas de Comunicaciones Extremo a Extremo, OEA

elementos, servicios y aplicaciones de red para detectar, predecir y corregir vulnerabilidades de seguridad.

La arquitectura de seguridad lógicamente divide un conjunto complejo de características relacionadas a la seguridad de red de extremo a extremo en componentes arquitectónicos separados. Esta separación permite un enfoque sistemático de la seguridad de extremo a extremo que puede ser usado para planificar nuevas soluciones de seguridad al igual que para determinar la seguridad de las redes existentes. Se abordan tres componentes arquitectónicos: dimensiones de seguridad, niveles de seguridad y planos de seguridad.

Dimensiones de Seguridad, una dimensión de seguridad es un conjunto de medidas diseñadas para abordar un aspecto particular de seguridad de red. Esta Recomendación X.805 identifica ocho de estos conjuntos que protegen contra todas las principales amenazas de seguridad. Las dimensiones de seguridad son:

1. Control de acceso
2. Autenticación
3. No-repudiación
4. Confidencialidad de la información
5. Seguridad de la comunicación
6. Integridad de la información
7. Disponibilidad
8. Privacidad

Niveles de Seguridad, para proveer una solución de seguridad de extremo a extremo, las dimensiones de seguridad deben ser aplicadas a una jerarquía de equipo de red y agrupamientos de instalaciones, a las que nos referimos como niveles de seguridad. La Recomendación X.805 define tres niveles de seguridad:

1. Nivel de Seguridad de la Infraestructura
2. Nivel de Seguridad de los Servicios
3. Nivel de Seguridad de las Aplicaciones

Los niveles de seguridad son una serie de factores que permiten soluciones de redes seguras: el nivel de la infraestructura habilita al nivel de los servicios y el nivel de los servicios habilita al nivel de las aplicaciones. Los niveles de seguridad identifican los lugares donde la seguridad debe ser abordada en productos y soluciones, proveyendo una perspectiva secuencial de seguridad de red.

Planos de Seguridad, un plano de seguridad es un cierto tipo de actividad de red protegida por dimensiones de seguridad. La Recomendación X.805 define tres planos de seguridad para representar los tres tipos de actividades protegidas que tienen lugar en una red. Los planos de seguridad son:

1. Plano de Administración
2. Plano de Control
3. Plano del Usuario Final

Estos planos de seguridad abordan necesidades de seguridad específicas asociadas con actividades de administración de la red, control de red o señalización de actividades y actividades del usuario final, respectivamente.

La Recomendación X.805 resume las dimensiones de la arquitectura de seguridad con la siguiente figura 6:

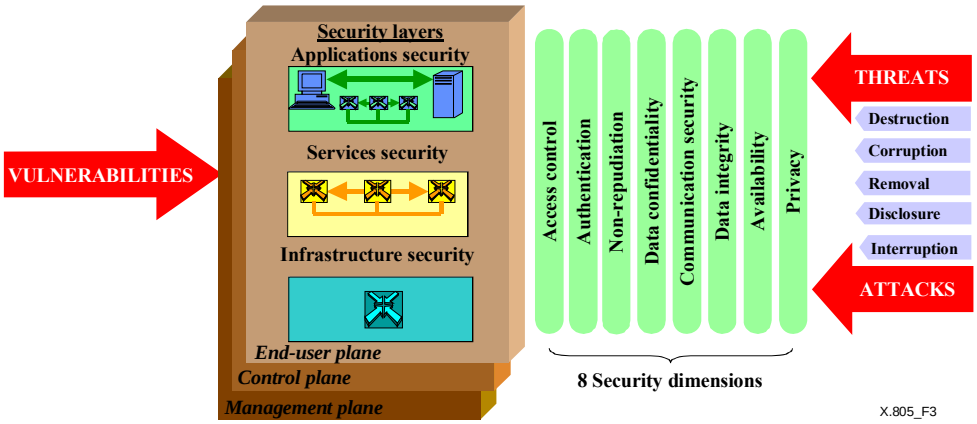


Figura 6 Arquitectura de seguridad para seguridad de red de extremo a extremo

La arquitectura de seguridad descrita en la Recomendación X.805 puede ser usada para guiar el desarrollo de definiciones de políticas de seguridad exhaustivas, planes de respuesta a incidentes y de recuperación y arquitecturas de tecnología, tomando en consideración cada dimensión de seguridad en cada nivel y plano de seguridad durante la fase de definición y planificación. La arquitectura de seguridad también puede ser usada como la base de una evaluación de seguridad que examinaría cómo la implementación del programa de seguridad aborda las dimensiones, niveles y planos de seguridad, a medida que se expiden políticas y procedimientos y se despliega la tecnología.

Una de las razones principales para buscar la seguridad en las telecomunicaciones es el propio concepto de privacidad, algo que se conoce comúnmente como el derecho

que tiene cada persona para controlar quién recopila y almacena información relacionada con ella, qué tipo de información y quién tiene acceso a ésta. Además, este concepto tiene que ver con los medios técnicos necesarios (por ejemplo, la criptografía) para garantizar que la información sólo llegue a los destinatarios deseados, de tal manera que solamente aquellas partes explícitamente autorizadas puedan recibirla e interpretarla.

La autenticación consiste en probar la veracidad de la identidad reclamada por una entidad. En este contexto, se consideran entidades no solamente a las personas sino también los mecanismos, servicios y aplicaciones. Con la autenticación se pretende también garantizar que una entidad no esté tratando de usurpar una identidad o de emitir una respuesta no autorizada a una comunicación previa. Existen dos tipos de autenticación, a saber la autenticación de origen de datos (es decir aquella necesaria en caso de asociación orientada a la conexión) y la autenticación de entidad par (es decir, aquella presente en una asociación sin conexión).

La red debe garantizar que se establece un intercambio de datos con la entidad par destinataria (y no con una que trate de suplantar la identidad o de responder a una comunicación previa) y que el origen de los datos sea el que se reclama. En general, tras la identificación viene la autenticación. La red debe proteger la información que se utiliza para la identificación, la autenticación y la autorización.

Integridad de datos, propiedad que consisten en que los datos no han sido alterados de una manera no autorizada. Además, la integridad de los datos garantiza que la información esté protegida contra las siguientes operaciones no autorizadas: modificación, supresión, creación, y copia de los datos. Se proporciona también un indicador de estas actividades no autorizadas.

No repudio, capacidad de evitar que un usuario niegue más adelante haber efectuado una acción. Entre éstas se incluyen la creación, origen, recepción y entrega de contenidos, por ejemplo envío o recepción de mensajes, establecimiento o recepción de llamadas, la participación en conferencias de audio y vídeo, etc.

Gracias a los requisitos de no repudio que se imponen, es posible colectar pruebas infalsificables del envío y/o recepción de datos a fin de evitar que el remitente niegue haber enviado un mensaje o el destinatario haberlo recibido. En la red se puede implementar esta característica mediante cualquiera o ambos de los dos métodos siguientes: se suministra a quien recibe la información prueba del origen de ésta, de tal manera que el remitente no pueda negar haberla enviado o rehusar su contenido; se

proporciona al remitente una prueba de la entrega de los datos, de tal manera que el destinatario no pueda negar más adelante haberlos recibido.

Además de la privacidad y la confidencialidad de datos, la autenticación, la integridad y el no repudio, esta recomendación define otras tres dimensiones de seguridad: control de acceso, seguridad de la comunicación, y disponibilidad.

La dimensión de seguridad del control de acceso protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones.

CENTRO DE COMPUTO.

La sala de computación o centros de cómputos son espacios físicos que cumplen con las condiciones mínimas para albergar equipos tecnológicos que permiten el uso de las tecnologías de información, es decir, son el centro tecnológico de las organizaciones que usa tecnología de información para el desarrollo de su negocio.

Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados. Hasta hace algunos años la exposición de los Equipos de Cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo y sabotaje.

Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo.

Otra precaución que se debe tener en los Centro de Cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.

El acceso al Centro de Cómputo debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carnet de identificación siempre en un lugar visible. Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.

Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.

El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.

Establecer políticas de control de entrada y salida del personal , así como de los paquetes u objetos que portan.

Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse algún componente.

Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados. Para protegerlos se debe tener en cuenta que: La temperatura no debe sobrepasar los 18º C y el limite de humedad no debe superar el 65% para evitar el deterioro.

Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Recomendaciones para el mantenimiento de Cintas Magnéticas y Cartuchos.

Las cintas magnéticas y cartuchos deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada.

Cintas Magnéticas:

a. La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

Temperatura : 4ºC a 32ºC

Humedad Relativa : 20 % a 80 %

b. El ambiente debe contar con aire acondicionado.

c. Las cintas deben colocarse en estantes o armarios adecuados.

d. Deberá mantenerse alejados de los campos magnéticos.

e. Se les debe dar un mantenimiento preventivo en forma periódica.

Cartuchos:

a. La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

Temperatura : 16ºC a más

a. Humedad Relativa : 20 % a 80 %

b. La temperatura interna del Drive puede oscilar entre: 5ºC a 45ºC.

c. Deben ser guardados dentro de su caja de plástico.

d. Deben mantenerse alejados de campos magnéticos.

Mantener las Áreas Operativas Limpias Y Pulcras

Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas, para enunciarlas aquí. Sin embargo, algunos de los problemas que usted puede evitar son: el peligro de fuego generado por la acumulación de papeles bajo el falso piso, el daño potencial al equipo por derramar el café, leche o chocolate en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, el peligro por fumar y las falsas alarmas creadas por detectores de humo. Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza.

Medidas Externas

Para finalizar nuestro trabajo expondremos las medidas para la protección de la información contenida en los sitios Web de las instituciones financieras o debilidades Externas.

La exposición más visible de las organizaciones financieras esta asociada a su presencia en la Internet a través de los servicios relacionados con sus paginas Web (banca en línea o sitio Web), estos sitios Web están construidos en dos módulos o núcleos, el primero son paginas que contienen información variada (servicios, productos, historia de la organización, ubicación de las agencias, cajeros automáticos, etc.) de la organización que es de carácter publico, es decir, pueden ser visualizadas por cualquier visitante (internauta) y el segundo modulo que son paginas de carácter transaccional (operaciones financieras) que solo pueden ser utilizadas por los usuarios autorizados de las instituciones y a las cuales tienen acceso a través de cualquier mecanismo de autenticación.

La primera amenaza de los sitios WEB es la denegación de servicios (DoS). En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computación o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad por la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación".

Los ataques de denegación de servicios (DoS) tiene varias modalidades las cuales son:

Consumo de ancho de banda, es la forma más insidiosas de los ataques DoS, los atacantes consumirán todo el ancho de banda (es la anchura, medida en hercios, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal) disponible de la red. Este tipo de ataques tiene dos escenarios: 1) los atacantes son capaces de inundad la conexión de red de la victima porque tienen más ancho de banda disponible. Un escenario probable es alguien que tiene una conexión T1 (1,544 Mbps) u otra conexión más rápida, que inunda un enlace de red de 56 Kbps o 128 Kbps. Equivale al choque frontal de un tren con un triciclo; 2) El llamado “DDoS (siglas en inglés de Distributed Denial of Service, denegación de servicio distribuida) es una ampliación del ataque DoS, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos. El invasor

consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del flood o saturación de información, pudiendo darse casos de un ataque de cientos o millares de computadoras dirigidas a una máquina o red objetivo

Un segundo tipo de ataque es por inanición de recursos. “Un ataque por inanición de recursos (resource-starvation) difiere del ataque de consumo de ancho de banda en que está enfocado más al consumo de recursos del sistema que al de recursos de red. Generalmente, este consumo de recursos está dirigido a la saturación del CPU, memoria, cuotas del sistema de archivos u otros procesos del sistema”25. Normalmente este tipo de ataque provoca un fallo general del sistema, o que se llene un disco de log, o procesos que se cuelgan porque necesitan CPU que el sistema no le está proporcionando o se lo proporciona escasamente.

Un tercer tipo de ataque DoS es por los defectos de programación. Los defectos de programación (programming flaws) son los fallos de una aplicación, sistema operativo o chip lógico que le impiden manejar condiciones excepcionales. Estas condiciones ocurren cuando un usuario envía datos imprevistos al elemento vulnerable. Muchas veces, los atacantes enviarán paquetes RFC (normas de definición del protocolo) anormales al sistema objetivo para determinar si la pila de red será capaz de manejar esta excepción o si acabará en un caos y con la caída de todo el sistema.

Un cuarto tipo de ataque son los ataques DNS y de enrutamiento. Un ataque DoS basado en enrutamiento consiste en que los atacantes manipulan la tablas de distribución o enrutamiento para denegar el servicio a redes o sistemas legítimos. La mayoría de los protocolos de enrutamiento como RIP (Routing Information Protocol) o BGP (Border Gateway Protocol) carecen de autenticación, o tienen una muy sencilla”. Se trata, por tanto, de un escenario perfecto para que cualquier atacante pueda alterar las rutas correctas y, falsificando su IP origen, crear una condición DoS. Las víctimas de estos ataques verán como su tráfico se dirige por ejemplo hacia un agujero negro: a una red que no existe.

Los ataques DoS sobre servidores de nombres de dominios (DNS) son tan problemáticos como los anteriores. Estos ataques intentan convencer al servidor DNS, por ejemplo, para almacenar direcciones falsas en la caché, cuando un servidor DNS

[25] Hachers, Secretos y Soluciones para la Seguridad de Redes, Stuart McClure

realiza una búsqueda el atacante puede redireccionar al sitio Web que prefieran o bien a un "agujero negro".

Contramedidas

Las contramedidas se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en su entorno. Por ejemplo, una organización de productos electrónicos frágiles puede aplicar contramedidas de seguridad física como fijar la maquinaria a los cimientos del edificio o agregar mecanismos de amortiguación. Estas contramedidas reducen la posibilidad de que un terremoto pueda causar daños físicos a sus bienes. Una vez aplicadas todas las contramedidas para reducir las amenazas y vulnerabilidades, sólo quedan riesgos residuales

Para las vulnerabilidades descriptas anteriormente, desafortunadamente, no hay maneras efectivas de evitar ser una víctima de un ataque DoS o DDoS, pero hay pasos que proponemos para reducir la probabilidad de un ataque:

1) Entrega en Outsorcing el hospedaje de la pagina Web informativa a un proveedor de servicios de Internet que posea capacidad tecnológica (servidores con suficiente poder de cómputos, anchos de bandas robustos (un E1, como mínimo)), es importante resaltar que algunas instituciones financieras han colocado sus sitios Web, fueran del país, buscado mejores tiempo de respuestas y seguridad. La utilización de un buen proveedor de Internet, minimiza los posibles ataques de denegación de servicios por consumo de ancho de banda.

2) Mantener actualizado los sistemas, aplicando los parches destinados a eliminar vulnerabilidades.

3) Los administradores deben filtrar todos los puertos, dejando únicamente operativos aquellos que sean estrictamente necesarios.

4) Disponer de una política de implantación y actualización de sistemas antivirus y software para detección de intrusos.

5) Instalar un cortafuego (firewall), y configurarlo para restringir el tráfico entrante y saliente del sitio Web.

Desde el punto de vista interno el establecimientos de medidas de seguridad es más complejo, como norma general, cuanto más alto sea el nivel de seguridad de una organización, más costosa resultará su implementación y más posibilidades habrá de que se reduzca su funcionalidad. Tras evaluar los posibles riesgos, quizá tenga que reducir el nivel de seguridad para conseguir aumentar la funcionalidad y reducir el costo.

En ocasiones, los niveles adicionales de seguridad darán como resultado sistemas más complejos para los usuarios. Un banco en línea puede decidir utilizar varios niveles de autenticación para sus usuarios cada vez que estos tengan acceso a su cuenta. No obstante, si el proceso de autenticación es demasiado complicado, algunos usuarios ni siquiera se molestarán en utilizar el sistema, lo que podría llegar a resultar más costoso que los ataques que el banco puede sufrir.

CONCLUSIONES

La gente sabe que la información es uno de los activos más importante de la compañía y por eso hoy las organizaciones están preocupadas en protegerla. Como es un elemento muy valioso la información es la más atacada. Y además, como es mayoritariamente digital, el nivel de exposición que tiene ese riesgo es aun más alto que el que podría hacer hace 10 años atrás. La gerencia sabe perfectamente que la TI es una diferencial en la competencia. El sector financiero fue el que antes emprendió el camino al darle seguridad a los bancos. Hoy el nivel de competencia entre bancos requiere que la mayoría de los servicios que una entidad da a sus clientes sea dado en tiempo real.

Hay que disponer sistemas y esto trasciende las paredes de un edificio, lo físico y requiere que se implementen mecanismos de protección de la información, tanto del usuario como de la entidad financiera. Es un segmento donde la competencia es muy alta y requiere de tecnología para brindar servicios sofisticados, la seguridad absoluta en los sistemas no existe, la mejor protección es conocer cuales son nuestras debilidades o brechas y mitigar as mismas con los procedimientos o recursos tecnológicos más apropiados.

Para bien de los tecnólogos hay una serie de recomendaciones y estándares que facilitan la gestión de seguridad de la información, mientras más próximo nuestra organización cumpla con dichas normas, menor será nuestra posibilidad de ser afectado por eventos tecnológicos.

Al finalizar dicho trabajo muchas de las brechas analizadas ya serán tema del pasado y estaremos enfrentado nuevas formas de ataques o vulnerabilidades, motivo por el cual es necesario una constante actualización de los mecanismos de seguridad de nuestras organizaciones.

BIBLIOGRAFÍA

Bibliografía Referenciada

25) STUART McCLURE, JOEL SCAMBRAY, “Hachers, Secretos y Soluciones para la Seguridad de Redes” editorial McGRAW-HILL, 2000.

ECHENIQUE GARCÍA, JOSE ANTONIO, “Auditoria en Informática”, editorial McGraw_Hill, edicion 2, 2002.

23) CHARLES CRESSON WOOD, ”Mejores Practicas Internacionales”, Políticas De Seguridad Informática, NETIQ, 2006

Bibliografía Examinada

DEL ROSARIO ZULEYMA, Peñalosa Santalla, “Guía para la Elaboración Formal de Reportes de Investigación” UCAB, Caracas 2006**.**

BALESTRINI ACUÑA, Mirian. “Como se elabora el proyecto de investigación”. Sexta Edición. BL Consultores. Caracas. (2002)

JOHN RAY, “TCP/IP”; traducción Luís del Pino González, Santiago Fraguas --Madrid Prentice Hall, 1999 . Edición. Especial.

HARVEY M. Deitel, “Introducción a los sistemas operativos “ ; versión en español de Roberto Escalona García ; con la colaboración de Iñaki Alegría Loinaz, Alberto Lafuente Rojo y Clemente Rodríguez Lafuente --Buenos Aires : Addison-Wesley Iberoamericana, 1999 . 2 Edición

MICROSOFT. “Guía de seguridad de Windows Server 2003”

MICROSOFT “Soluciones de Seguridad, Soluciones de Administración”. 2004

MICROSOFT “Windows 2000 Active Directory Services” Curso oficial de certificación MCSE, editorial McGrawHill

Leyes o Reglamentos

14) Normas para una Adecuada Administración Integral de Riesgos, Superintendencia de Bancos y Otras Instituciones Financieras, Resolución Bancaria 136.03 publicada el 3 de Junio de 2003 en la Gaceta Oficial N° 37.703.

18) Ley Especial sobre los Delitos Informáticos, Republica Bolivariana de Venezuela, Caracas 2001.

20) Ley sobre Mensajes de Datos y Firmas Electrónicas, Republica Bolivariana de Venezuela 2001.

Presentaciones o Charlas

10) ORACLE-HP-Deloitte, Basilea II, Adaptar, Adoptar o Peder, CD con presentaciones sobre el impacto de Basilea II en el sistema Financiero, Caracas mayo 2007.

15) Presentación en las III Jornadas de "Delitos Informáticos"- SUSCERTE – Caracas-Venezuela-2006

19) Las fronteras de la Ley / Lorenzo Lara Carrero, compilador --Caracas : [CAVECOM-E], 1999.

Paginas WEB

1**) Introducción a la Criptografía**, trabajo sobre la historia de la técnica de criptografía utilizada desde la antigüedad hasta los métodos actuales, están información se encuentra en la URL siguiente,
http://rinconquevedo.iespana.es/rinconquevedo/criptografia/introduccion.htm
consultada en septiembre del 2007.

4) **Philip R. Zimmermann,** es el creador de Pretty Good Privacy (algo así como Muy Buena Privacidad), un paquete software para la encriptación de correo electrónico. Originalmente diseñado como una herramienta para los derechos humanos, PGP se publicó gratis en la Internet en 1991, la pagina web donde se encuentra la información es: http://www.philzimmermann.com/ES/background/background.html, revisión septiembre del 2007.

5) **Enciclopedia de Virus**, Virus Informáticos desde la A –Z, sitio web que posee información variada sobre los virus y otras amenazas en la RED, la dirección es:
http://www.enciclopediavirus.com/enciclopedia/articulo.php?id=20, fecha de revisión septiembre del 2007.

6) **Revista Pc-News.com**, Revista especializada en temas de computación, en la cual se publican Artículos de Diferentes Autores, El tema es de la Integración vendrá la innovación, el sitio web es:
http://www.pc- nws.com/detalle.asp?sid=&id=11&Ida=1926 , fecha de revisión septiembre del 2007

7) **Revista Pc-News.com**, Revista especializada en temas de computación, en la cual se publican Artículos de Diferentes Autores, el tema es Definiendo "Seguridad de la Información", de la consultora Espiñeira, Sheldon y Asociados
http://www.pc- nws.com/detalle.asp?sid=&id=11&Ida=1926 , fecha de revisión septiembre del 2007

12) **Banco Nacional de Crédito**, Unidad de Administración Integral de Riesgo, información referente a manejo y gestión del riesgos, intranet de la Institución, fecha de revisión mayo 2007.

16) **Encuesta realizada por la Univesidad Carnegie Mello** y los servicios secreto de los EEUU, sobre el estado de la seguridad y el delito Informático, el los estados unidos, el sitio web es: http://www.cmu.edu/research/index.shtml, revisión septiembre del 2007.

17) **La Ley Sarbanes-Oxley**, nació como respuesta a una serie de escándalos corporativos que afectaron a empresas estadounidenses a finales del 2001, producto de quiebras, fraudes y otros manejos administrativos no apropiados, que mermaron la confianza de los inversionistas respecto de la información financiera emitida por las empresas. Así, en Julio de 2002, se aprobó la ley Sarbanes-Oxley. El texto legal abarca temas como el buen gobierno corporativo, la responsabilidad de los administradores, la transparencia, y otras importantes limitaciones al trabajo de los auditores. En el siguiente sitio se tomo la información:
http://www.deloitte.com/dtt/section_node/0,1042,sid%253D96325,00.html, revisión septiembre 2007

21) **Revista Pc-News.com**, Revista especializada en temas de computación, en la cual se publican Artículos de Diferentes Autores, el tema es "Brechas de Seguridad y Controles de Seguridad en las Empresas Venezolanas", de la consultora Espiñeira, Sheldon y Asociados, el sitio web es:
http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=2288, fecha de revisión septiembre del 2007

22) Sitio Web con información referente a temas de seguridad, especializados en Tecnología Windows y Linux, los autores de este articuló es la empresa Sombra Team, que adicionalmente son proveedores de Hosting, la pagina web es:
http://www.xombra.com/go_normal.php?articulo=114

24) **OEA**, Comisión Interamericana de Telecomunicaciones, "ARQUITECTURA DE SEGURIDAD PARA SISTEMAS DE COMUNICACIONES EXTREMO A EXTREMO", Documento Coordinado de Normas Nro. 7 : ,2004

ANEXO 1

MANUAL DE SEGURIDAD DE ACTIVOS DE INFORMACIÓN

Introducción Manual

Objetivos Generales

Establecer las normas, políticas y prácticas de seguridad que garantice la Integridad de los Activos de Información del Banco X.

Objetivos Específico:

El manual está estructurado en cuatro (4) secciones donde se expresa las normas de protección de la información relacionadas con

Seguridad Lógica

Seguridad Administrativa

Seguridad Física

La revisión y actualización de este documento, es responsable de la Gerencia de Seguridad de Datos del Banco X, la cual estará alerta para hacer efectiva las mejoras y adiciones que estas normativa requieran de acuerdo a las nuevas realidades y cambios que surjan en el Banco

Enunciado de la Política de la Seguridad de Activo de Información

La información se ha convertido en un instrumento de operación, capaz de redefinir empresas, y fomentar la creación de otras nuevas, crear productos y desarrollar mercados. Si bien es cierto que el intercambio en sí es un factor que contribuye a mayor entendimiento del trabajo y conduce a una mayor facilidad y eficiencia en su realización, existe información que por la naturaleza de su contenido exige un tratamiento de reserva.

Banco X, está expuestas a un entorno agresivo que hace codiciable su información confidencial, por lo que es imprescindible en nuestra actividad protegerla mediante todos los medios a nuestro alcance, a fin de mantener la confidencialidad, integridad y disponibilidad de la información contenida en cualquier medio oral, impreso, visual y electrónica.

Esta tarea ha sido definida por la Gerencia de Seguridad de Datos, la cual tiene como fundamento la siguiente política:

“Es deber de todos los usuarios de Activos de Información del Banco X, asegurar que toda la información propiedad de la empresa o cedida a ella sea protegida en forma cónsona con su clasificación, valor que representa y su potencial de pérdida

por hurto, apropiación indebida, destrucción, manipulación y/o divulgación no autorizada”

Advertencias

Cualquier violación a estas disposiciones es contraria a las prácticas del negocio e implica sanciones que pueden variar dependiendo de la importancia de la política incumplida desde el punto de vista de la seguridad y control del ambiente de tecnología de información del Banco.

1. Política de Seguridad

1.01 Política de Seguridad Informática

1.01.01 Documento de Política de Seguridad Informática

1. Protección de la Información

La información debe ser protegida de acuerdo con su confidencialidad, valor y criticidad

2. Uso de la Información

La información del Banco X debe ser usada únicamente para los propósitos de negocios Banco expresamente autorizado por la gerencia.

3. Manejo, Acceso y Uso de la Información

La información es un activo vital y todos los accesos, uso y manejo de la información del Banco X deben y ser consistentes con sus políticas y normas.

4.Las excepciones a las políticas de seguridad deben ser autorizadas por las vicepresidencias o gerencias propietarias de la información.

5.El hecho de que las vice-presidencias o gerencias no hagan cumplir algún requerimiento de las políticas no significa que otorga su consentimiento.

6. Infracción a las Políticas

La gerencia del Banco X puede considerar el enjuiciamiento o terminación de la relación laboral cuando las infracciones a las políticas sean consideradas como faltas graves.

7. Revocación de Privilegios de Accesos

El Banco X se reserva el derecho de revocar los privilegios sobre tecnología informática al usuario en cualquier momento.

1.01.02 Revisión y Evaluación

8. Cumplimiento Forzoso de los Controles de Seguridad

Todos los sistemas de control de la seguridad informática deber ser susceptibles de cumplimiento forzoso antes de adoptarse como parte normal del proceso operativo.

2.Seguridad Organizacional

2.01 Infraestructura de la Seguridad Informática

9. Alteración No Detectada de la Información

La gerencia debe establecer y mantener las medidas de seguridad, prevención y detección necesaria para garantizar que la información del Banco X está protegida del riesgo de alteraciones no detectadas.

10. Comité de Gestión de Seguridad Informática

Un comité de Gerencial de Tecnología, compuesto por la alta gerencia o los delegados de cada división del Banco X, deben reunirse por lo menos una vez al trimestre para revisar el nivel actual de seguridad informática, revisar los procesos de monitoreos de las incidencias de seguridad del Banco X, aprobar políticas nuevas ó modificar las existentes; y realizar otras actividades gerenciales de alto nivel necesarias para mantener la seguridad informática

2.01.01 Coordinación de Seguridad Informática

11. Riesgo Significativos para la Seguridad Informática

Por cada riesgo importante para la seguridad de los sistemas informáticos, la gerencia debe tomar una decisión específica acerca del extremo al que está dispuesta a llegar el Banco X para aplicar su propio seguro y aceptar el riesgo, buscar cobertura o mitigar la misma.

12. Control de Nuevas Tecnologías

En cada instancia donde se utilice nueva tecnología en un sistema informático de producción del Banco X, las operaciones de controles y seguridad asociados a la nueva tecnología deben ser particularmente rigurosos hasta que se demuestre que la nueva tecnología es confiable, rápidamente controlable y que es un verdadero apoyo a las actividades del negocio.

13. Inhabilitación de Componentes Críticos de Seguridad

Los componentes críticos de la infraestructura de seguridad informática del Banco X, no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la Gerencia de Seguridad de Datos

14. Evaluación del Riesgo en los Sistemas de Producción

Todos los sistemas computarizados de producción deben ser evaluados periódicamente por la Gerencia de Seguridad de Datos para determinar el mínimo conjunto de controles requeridos para reducir y mantener el riesgo a un nivel aceptable

2.01.02 Asignación de Responsabilidades

15. Definición de Propietarios de la Información

Cada vicepresidencia y/o Gerente responsable de área determinada del Banco X, deberá establecer claramente la asignación de responsabilidades de propiedad para las bases de datos, archivos maestro o cualquier otro repositorio de información compartido.

16. Asignación de la Propiedad de la Información

La Gerencia Ejecutiva debe asignar la responsabilidad de la propiedad a un único individuo interno que haga el mayor uso de la información.

17. Responsabilidad de la propiedad de los Departamentos

Con excepción de la información operacional relativa a los computadores y a la red, la Gerencia de Operaciones no debe ser Propietario de ninguna información.

18. Propiedad Predeterminada de la Información

Si la propietaria de un tipo específico de información residente en un computador multiusuario de producción no ha sido claramente asignada a un gerente específico, recaerá temporalmente en el Gerente de Operaciones

19. Delegación de la Propiedad de la Información

La responsabilidad de especificar controles de información no debe ser delegada a proveedores de servicios ajenos al Banco X.

20. Revocación a los Privilegios de Acceso a los Sistema del Banco X.

La Gerencia de Área de Seguridad de Datos, debe revocar los privilegios de acceso a los sistemas de información computarizado inmediatamente que el empleado (fijo, temporal, contratado, contratista, asesor, pasante y demás) deje de prestar servicio al Banco X, tenga ausencia prolongada, ó sea transferido de área. Esta actividad debe estar coordinada con la Vice-presidencia del Área de Recursos

Humanos, a fin de obtener los últimos cambios en la organización relacionados con los empleados.

21. Enfoque Gerencial de la Seguridad

La Gerencia debe garantizar que la seguridad informática dentro de cada departamento sea tratada como un problema organizacional normal a ser afrontado y resuelto, siendo la misma gerencia responsable de promover la seguridad como problema de todos.

22. Seguridad Informática Centralizada

La orientación, dirección y autoridad de las actividades de seguridad informática están centralizadas en la Gerencia del Área de Seguridad de Datos.

23. Responsabilidades del Departamento de Seguridad de Datos

El departamento de Seguridad de Datos es responsable de establecer y mantener las políticas, normas, lineamientos y procedimientos relativos a la seguridad informática de toda la organización.

24. Tarea del Departamento de Seguridad de Datos

La Gerencia de Seguridad de Datos debe proporcionar direcciones técnicas para garantizar que la información del Banco X esté protegida con procesos que mantenga la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas que la mantienen

25. Normas y Procedimientos del Área de Seguridad de Datos

La Gerencia de Seguridad de Datos tiene la facultad para crear y periódicamente modificar las normas técnicas y los procedimientos operativos que regula el tema de seguridad dentro de la Organización.

26. Planes de Seguridad Informática

Junto con la gerencia correspondiente, la Gerencia de Seguridad de Datos debe preparar planes anuales para el mejoramiento de la seguridad de todos los sistemas informáticos del Banco X.

27. Misión del Departamento de Seguridad de Datos

La Gerencia de Seguridad de Datos es responsable de evitar perder o comprometer los recursos informáticos críticos, valiosos y sensibles al Banco X, a través de la coordinación y dirección de las acciones específicas que proporcionen un ambiente informático seguro y estable, consistente con las metas y objetivos del Banco X.

28. Manual de Seguridad de Datos

El Departamento de Seguridad de Datos debe preparar, mantener y distribuir uno o más manuales de seguridad de informática que describan con exactitud las políticas, las normas y los procedimientos de seguridad informática del Banco X.

29. Evaluación de Riesgo

La evaluación de los riesgos en seguridad informática debe ser realizada por terceros no interesados.

30. Recursos para la Seguridad Informática

La Gerencia debe suministrar suficientes recursos y atención al personal para poder ocuparse adecuadamente de la seguridad de los sistemas informáticos.

31. Autorización para Cambios de los Sistemas Informáticos

Los Gerentes de Áreas u otros integrantes del equipo gerencial no pueden firmar contratos, iniciar proyectos internos ni de otra manera comprometer al Banco X a efectuar modificaciones en sus sistemas de computación o de comunicación, a menos que tales modificaciones hayan sido autorizadas previamente tanto por el responsable principal del Área de Tecnología con la aprobación de la Vice-presidencia Ejecutiva de Administración y la participación de la Gerencia de Área de Seguridad de Datos

2.01.03 Inclusión de la Seguridad en la Responsabilidades del Cargo

32. En la descripción de cargos debe contener las especificaciones sobre la seguridad informática en donde los trabajadores tenga acceso a información confidencial, valiosa o crítica.

33. Evaluación de Desempeño

Se debe considerar el cumplimiento de las políticas y procedimientos de seguridad informática en todas las evaluaciones de desempeño de los empleados.

34. Antiguos Hackers y Delincuentes Reformados

Banco X no debe emplear antiguos hackers ni delincuentes reformados para trabajar en seguridad informática o realizar trabajos forenses.

35. Aumento Significativo de Riqueza

En caso de que un trabajador del Banco X demuestre un inexplicable aumento de riqueza, la gerencia tiene el deber de investigar discretamente el origen de dicha riqueza.

36. Derecho de Propiedad

Sin excepciones específicas escritas, todas los programas y documentación generados o proporcionados por cualquier trabajador en beneficio del Banco X son propiedad del Banco X y todos los trabajadores que proporcionen tales programas o documentación deben firmar una declaración a tal efecto, previa a la entrega de dicho material.

2.01.04 Adiestramiento de Usuario

37. Educación y Adiestramiento en Seguridad Informática

Los usuarios no deben tener acceso a los sistemas informáticos del Banco X, a menos que hayan leído la Políticas de Seguridad de Activos de Información y tomando un pequeño examen que demuestre claramente que entienden el material en dicha política.

38. Políticas y Procedimientos Relativos a la Privacidad

Con excepción de los relativos al manejo de datos privados de las personas, las políticas y procedimientos de seguridad informática deben ser revelados sólo a los trabajadores del Banco X y a terceros seleccionados, tales como los auditores, quienes tienen una necesidad legítima de negocio sobre esta información.

39. Adiestramiento en INTERNET

Los trabajadores pueden acceder a Internet a través de los servicios del Banco X sólo si han sido autorizados por la gerencia del departamento y han completado un curso de adiestramiento en políticas y prácticas de Internet.

40. Adiestramiento Básico

Los trabajadores deben haber terminado satisfactoriamente todos los otros adiestramientos básicos necesarios para efectuar su nuevo trabajo antes de recibir el adiestramiento de seguridad informática.

41. Adiestramiento en Seguridad Informática

Todos los trabajadores deben ser provistos con suficiente adiestramiento y material de referencia de soporte para permitirles proteger adecuadamente los recursos informáticos del Banco X.

42. Responsabilidad en Adiestramiento

La Gerencia de Seguridad de Datos debe proporcionar cursos de actualización y otros materiales, para recordar regularmente a los trabajadores sus obligaciones con respecto a la seguridad informática.

43. Tiempo de Adiestramiento

La Gerencia debe asignar tiempo hábil para que los trabajadores se familiaricen con las políticas de seguridad, procedimiento y otras formas de llevar los negocios en el Banco X.

44. Clases Sobre Seguridad Informática

Dentro de los tres meses siguientes a la fecha en que fue empleado en el Banco X, cada trabajador debe asistir a una clase de toma de conciencia respecto de la seguridad informática y firmar una declaración de entendido el material y que tuvo la oportunidad de hacer preguntas.

45. Adiestramiento Técnico y Educación Continua

Todo el personal técnico de los sistemas informáticos deben tener suficiente adiestramiento crítico se su trabajo, incluyendo seguridad, aseguramiento de la calidad y relaciones con el cliente.

46. Responsabilidad en la Seguridad Informática

La responsabilidad de la seguridad informática del día a día debe ser tarea de cada trabajador y no sólo de la Gerencia de Seguridad de Datos.

2.01.05 Clasificación de la Información

47. Propiedad de Archivos y Mensajes

El Banco X tiene la propiedad legal del contenido de todos los archivos y mensajes almacenados o transmitidos en sus computadores y sistemas de redes, y se reserva el derecho de acceder a esta información sin aviso previo cuando exista una necesidad genuina de negocios.

48. Clasificación de Datos en Cuatro Categorías

Uso y Procedimientos de Seguridad Informática

Toda la documentación referente a la Seguridad Informática del Banco X, inclusive, sin limitaciones, de las políticas, normas y procedimientos, deben ser clasificadas como “Sólo Para Uso Interno” a menos que haya sido expresamente creada para ser utilizada para procesos de negocios externo o por socios.

Todos los datos del Banco X deben ser divididos en las siguientes cuatro clasificaciones:

a. SECRETA: Se aplica a la información más sensible del negocio, cuyo propósito es estrictamente de uso interno del Banco X. Su divulgación no autorizada podría dañar seria y adversamente al Banco X, sus accionistas, socios o a sus clientes.

b. CONFIDENCIAL: Se aplica a la información de negocios menos crítica, pero aún importante para su uso en el Banco X. Su divulgación no autorización podría impactar negativamente en el Banco X, sus accionistas, sus socios o sus clientes.

c. PRIVADA: Se aplica a información personal que se ha de usar en el Banco X. Su divulgación no autorizada podría impactar seria y negativamente al Banco X y a sus empleados.

d. NO CLASIFICADA: Se aplica a cualquier otra información que no corresponda a las tres clasificaciones anteriores. Si bien su divulgación no autorizada va contra la política, no se espera que tenga un impacto serio o adverso sobre el Banco X, sus empleados, accionistas, socios y clientes.

49. Clasificación de la Información Según los Niveles de Confidencialidad

Si un sistema contiene información y recursos con diferentes niveles de confidencialidad las cuales no pueden ser controladas independientemente, las medidas de protección acordadas deben estar al máximo nivel de confiabilidad establecida.

50. Lineamentos Para la Información Secreta Confidencial y Privada

Los empleados del Banco X, deben proteger la información identificada como secreta y privada, contra la divulgación y uso no autorizado. Los propósitos internos y los secretos de negocios del Banco X, son clasificados como información confidencial. La intención de esta política es fomentar que toda aquella información de revista, catalogada como “secretos del negocio” debe manejarse a través de convenios de confiabilidad apropiada y no divulgarse a terceros sin la autorización de la Vice-presidencia o Gerencia propietaria de la información.

2.01.06 Cuándo Utilizar la Encripción

51. Utilización de Procesos de Encripción

No deben ser utilizados procesos de encripción, a menos que sean autorizados por la Gerencia de Seguridad de Datos. Asimismo, deben utilizarse algoritmos estándares aprobados para tal fin.

52. Prohibición de Utilitarios de Encripción que Utilicen Contraseñas o Claves Provista por los Usuarios.

A fin de prevenir la pérdida de información crítica del Banco X, los empleados del Banco X, no deben utilizar procesos de encripción que requieran una contraseña o clave provista por el usuario. Esto evitará que la información encriptada no pueda estar disponible debido al olvido, pérdida o retención intencional de la clave o contraseña por parte del usuario que la generó.

53. Encripción de la Información Confidencial

Siempre que se transmita información clasificada como confidencial a través de la red del Banco X, la misma debe ser previamente encriptada según los estándares aprobados antes de su envío. Asimismo, deben ser considerado los siguientes aspectos:

a. Cuando se maneje información confidencial en medio de almacenamiento electrónico que se puedan leer por computadoras, cinta magnéticas, CD-ROMs, disquetes, etc. se debe procurar que la misma permanezca en forma encriptada, a fin de prevenir revelaciones en caso de robo o utilización de dichos medios por parte de terceros.

b. Si la información clasificada como confidencial se encuentra en forma electrónica, debe estar bajo su forma cifrada cuando no se esté utilizando en forma activa; por ejemplo cuando no esté siendo manipulada a través de un software o revisada por un usuario autorizado.

54. Protección del Material Utilizado en la Encripción

Siempre que se utilice el proceso de encripción, el material utilizado para generar, distribuir y almacenar las claves (claves utilizadas para cifrar datos, claves maestra, papel carbón, cintas de impresoras, etc) y las versiones en papel de las claves, deben estar resguardadas cuando no se estén utilizando, a fin de evitar que las mismas sean reveladas a personas no autorizadas. Estas medidas de protección deben aplicarse durante todo el ciclo de vida de los activos de información

protegidos por esas claves, para evitar que el material utilizado para generar dichas claves sea accedidas por usuarios no autorizados. Todos los materiales utilizados para generar, distribuir y almacenar claves deben protegerse y no divulgarse a personas no autorizadas. Cuando estos suministros ya no sean necesarios, deben destruirse mediante el uso de máquinas trituradoras de papeles, incineradores u otros métodos autorizados, en presencia de un testigo del área de Seguridad Física. La destrucción de este material debe generar un acta de certificación.

55. Uso de Sistemas de Administración de Claves de Encripción Automáticas

Siempre que existan sistemas de Administración de claves de encripción comercialmente disponible, el Banco X debe procurar el uso de procesos automáticos para el cifrado de la información, en lugar de procesos manuales.

56. Divulgación de Claves de Cifrado – Controles

Las claves de cifrados deben protegerse de la divulgación no autorizadas a través de controles técnicos, tales como cifrados en claves separadas y la utilización de un hardware resistente a modificaciones.

2.02 Seguridad en el Acceso

2.02.01 Identificación de Riesgo Originados por Acceso

57. Uso de Perfiles de Usuarios y Contraseñas

Todo usuario del Banco X, requiere el uso obligatorio de un identificador de usuario y una contraseña para tener acceso al ambiente informático del Banco X. Así mismo, la función de Seguridad de Datos dentro de sus labores de administración, le define a cada usuario un código de identificación compuesto por un mínimo de seis (6) de caracteres y hasta un máximo de ocho (8)

En relación con las contraseñas, estas deben ser personales e intransferibles y cada uno de los usuarios es responsable por su uso y resguardo adecuado, de tal manera de preservar su confiabilidad.

Toda excepción de esta política debe ser documentada, asimismo quedará exceptuados los usuarios generados de manera automática al momento de instalación de un software, debido a que está establecido de esa manera con el proveedor. A continuación se presentan algunos de los usuarios que quedaran fuera de la política:

a. Interactive Voice Response (IVR), usuarios automáticos.

b. Cobranza, usuarios automáticos.

c. Producción (Operator, Scheduler)

d. Otros

58. Características de las Contraseñas

Todas las contraseñas de los sistemas de información computarizados del Banco X, deben tener las siguientes características:

a. Longitud mínima: Todas las contraseñas deben tener al menos seis (6) caracteres alfanuméricos

b. Re-utilización la contraseñas: ningún trabajador del Banco X podrá re-utilizar la previamente utilizada, a menos que hayan transcurrido 4 períodos de caducidad de la misma. Es de hacer notar que en la mayoría de las plataformas computacionales, este mecanismo de control es perfectamente configurable. Las excepciones de esta políticas deben estar debidamente justificadas y documentadas.

c. Caducidad de las contraseñas: las contraseñas deberán expirar cada 30 días calendarios. El sistema deberá advertir al usuario de esta situación. Las excepciones deberán estar debidamente justificadas y documentadas.

59. Lineamentos para la Creación de Contraseñas

Todas las contraseñas creadas por los empleados del Banco X para acceder a las redes y sistemas de información computarizados, deben ser difíciles de deducir, en tal sentido:

a. No deben ser utilizadas sucesiones de caracteres comunes, al igual que detalles personales tales como no nombre de esposa(o), número de cédula, fecha de nacimiento, etc., a menos que sean combinaciones con caracteres independientes.

b. Las contraseñas creadas por los usuarios, no deben formar parte del conjunto de palabras comunes al entorno del Banco X, por ejemplo: Banco, Nacional, Crédito.

c. Se debe procurar la mezcla de caracteres alfabéticos y no alfabéticos, mayúsculas y minúsculas.

d. No deben utilizarse contraseñas compuestas por ciertos números de caracteres cuyos cambios sean predecibles; es decir, contraseñas cíclicas y/o repetitivas. Generalmente estas contraseñas incluyen cambios basados en el mes, un proyecto o algún factor de fácil suposición que haya sido igual o similar a una contraseña utilizada con anterioridad. A discreción de la funciones de la Gerencia

de Seguridad de Datos, deben conducirse ejercicios de violación de contraseñas y mecanismos de protección de la información de los diferentes ambientes computarizados, a fin de determinar las anomalías presentes en este aspecto toma y las acciones pertinentes.

60. Reactivación de la Contraseña

El mecanismo de reactivación de contraseñas consistiría en la asignación del mismo identificador de usuario como contraseña por parte del personal. La Gerencia de Seguridad de Datos, activará la misma, la cual debe expirar automáticamente al ser utilizada la primera vez y por lo tanto, el usuario deberá cambiarla inmediatamente.

2.02.02 Manejo de Contraseña en Interfaces de Usuarios

61. Despliegue de Contraseña

El despliegue en pantalla de las contraseñas debe enmascararse u ocultarse, a fin de evitar que personas no autorizadas puedan visualizarlas y recuperarlas posteriormente.

62. Límite de Intentos errados de conexión

A fin de disminuir el riesgo de accesos no autorizados, el número de intentos consecutivos es ingreso de una contraseña incorrecta debe estar limitado. Después de tres (3) intentos fallidos de conexión, el perfil de usuario involucrado debe ser temporalmente deshabilitados hasta que el mismo sea restablecido por el personal de la Gerencia de Seguridad de Datos.

63. identificador de Usuario Administrador

Los administradores de sistema que manejan sistemas de computación con más de un usuario deben tener por lo menos dos identificadores de usuario, uno que le proporcione acceso privilegiado al sistema con su respectivo registro, y otro que le proporcione privilegios de un usuario normal, para facilitar su trabajo diario.

64. Acceso a Comando del Sistema Operativo

No se debe permitir que los usuarios finales utilicen comandos en el ámbito de sistemas operativos, mediante su limitación a los menús que muestran sólo aquellas funciones para las cuales han sido automatizados.

65. Actualización de Información de Producción

Los privilegios en sistemas deben definirse de modo tal que el personal no relacionado con el área de producción, incluyendo entre otros a auditores internos, administradores de seguridad informática, programadores y operadores de computadoras, no pueda actualizar la información de producción.

2.02.03 Manejo Interno de Contraseña

66. Contraseñas Iniciales

Las contraseñas emitidas por el Administrador de Seguridad deben estar vencidas, obligando así al usuario a seleccionar otra contraseña antes de completar el procedimiento de inicio de sección.

67. Almacenamiento de Contraseñas en forma legible

Las contraseñas son Activos de Información secretos, por lo tanto, las mismas no deben ser almacenadas en forma legible en los archivos de procesamiento por lote, procesos de accesos automáticos (log-in) en computadoras sin control de accesos u otros sitios donde no utilizadas puedan descubrirlas.

68. Encripción de Contraseñas

Las contraseñas siempre deben estar encriptadas cuando sean almacenadas por un largo período ó cuando sean transmitidas por la red. La intención de esta política es prevenir la revelación de contraseñas por interceptación del mensaje ó por manipulación de los “logs” del sistema por parte del personal técnico ó persona no autorizadas.

69. Prohibición de Incorporación de Contraseñas en Aplicaciones

A fin de permitir el cambio de las contraseñas cuando sea requerido, no deberán incorporarse las mismas en software desarrollado o modificados por empleados del Banco X en forma de código del programa.

70. Prohibición de la Recuperación de Contraseñas

Todos los equipos de computación y sistemas de comunicación del Banco X, deben estar diseñados, probados y configurados de manera adecuada, a fin de imposibilitar la recuperación de contraseñas

71. Proceso de autenticación de Usuarios provisto por los sistemas Operativos

Los procesos de autenticación de usuarios provisto por los sistemas operativos o software de control de acceso, deben ser el mecanismo de control inicial para acceder a los sistemas del Banco X. Cualquier otro proceso de autenticación

desarrollado e implantado por los empleados de la Institución debe ser consistente con el mecanismo de autenticación provisto por los sistemas operativos.

72. Cambios de las Contraseñas provista por un Proveedor

Todas las contraseñas por defecto suministradas por los proveedores de software y servicios Banco X deben ser cambiadas siempre que sea posible antes de que la Institución implante los sistemas en ambiente de producción/operación.

2.02.04 Responsabilidad del Usuario Relacionadas con la Contraseñas y Perfiles de Usuario

73. Requerimiento de Contraseña Diferente en Sistema Diferentes

En caso de que se utilicen esquema de diferentes perfiles y usuarios y contraseñas para los diferentes sistemas del Banco X, los usuarios deberán procurar el uso de contraseñas diferentes en cada uno de los sistemas a los cuales tienen acceso y abstenerse de usar la misma contraseña para los múltiples sistemas de la Institución.

74. Contraseñas Compartidas

Nunca de deben distribuir ni revelar las contraseñas a ninguna persona distinta al usuario autorizado incluyendo a terceros entre otros agregados de datos y servicios de resumen / formateo de datos. El incumplimiento de esta política será catalogado como falta grave.

75. Identificadores de Personales de Usuarios

Los usuarios deben responsabilizarse de toda la actividad realizada con sus identificadores personales de usuario y no deben permitir que otras personas realicen actividad con éstos ó que realicen actividades algunas con identificadores que pertenezcan a otros usuarios.

76. Compartir Códigos de Accesos

Las cuentas de computación, los identificadores de usuarios, las contraseñas de red, los números de identificación personal en la casilla de correo de voz, los números de tarjetas de créditos y otros códigos del Banco X, no deben utilizarlos ninguna otra persona distinta a aquélla para quien fueron emitidas originalmente.

77. Prueba de los Controles de Sistema de Informático

Los empleados no deben probar o tratar de comprometer los controles internos, a menos que la gerencia de Seguridad de Datos lo apruebe específicamente con antelación y por escrito.

78. Explotación de las Vulnerabilidades de la Seguridad de Sistema

Los usuarios no deben explotar los puntos vulnerables ó las deficiencias en la seguridad de los sistemas informáticos para dañar estos sistemas ó la información, obtener recursos de aquellos autorizados, quitar los recursos a otros usuarios u obtener accesos a otros sistemas de los que no han sido autorizados

79. Sesiones Activas Desatendidas

Si el sistema de computación al cual están conectados o el cual están utilizando contiene información sensible, los usuarios no deben dejar desatendido sus computadores personales, estaciones de trabajo o terminales sin salir del sistema o invocar un protector de pantalla.

2.02.05Uso del Sistema

80. Restricciones de Almacenamiento de Software no autorizados en los Equipos y/o Sistema de Comunicación

Los empleados Banco X no deberán almacenar, copiar o utilizar juegos y/o software en los equipos de computación y/o sistemas de comunicaciones del Banco X. Generalmente los juegos pueden estar infectados de virus informáticos así como también inciden en la distracción de los empleados en relación con sus actividades diarias, En tal sentido, la instalación de software debe ser realizada y/o autorizada por la Gerencia de Seguridad de Datos, sólo después de adquirida la licencia de uso, utilizando las fuentes originales del proveedor y llevando un control adecuado del número de instalaciones y licencias adquiridas.

81. Uso de los Sistemas de Información y/o Servicios de Comunicación del Banco X para Propósitos Personales

Sólo deben usarse los sistemas de información computarizados y/o servicios de comunicación del Banco X para fines de negocio. El uso personal solo es permitido bajo la autorización especial de las gerencias, en coordinación con la Gerencia de Seguridad de Datos, bajo las siguientes premisas:

a. Que sea ocasional

b. Que no consuma una cantidad considerable de recursos que pudieran ser utilizados para fines del negocio

c. Que no interfiera con la productividad del empleado

d. Que no incluya ninguna actividad comercial, tales como vender productos, hacer negocios, buscar empleo, etc.

e. Que no esté relacionada a actividades políticas

82. Usos Permisible de la Información del Banco X.

La información de Banco X sólo debe usarse para propósitos de negocios y su uso debe estar autorizado por las Unidades de Negocios. La intención de esta política es declarar, específicamente, que se prohíbe el uso no autorizado de la información de Banco X. En esta política, el enfoque está basado en el uso de la información, en lugar de los sistemas que manejan esta información. Esta política es complementada por la política de clasificación de la información

83. Revelación de Información de la Identificación de Usuario a Terceras Personas

Los empleados del Banco X no deberán proporcionar información de la identificación de usuarios para acceder a los sistemas de información computarizados y/o servicios de comunicación del Banco X a contratista, consultores o empleados temporales. En tal sentido, debe solicitarse a la Gerencia de Seguridad de Datos de manera expresa, la definición de los usuarios que requieran acceder a los recursos de computación del Banco X.

84. Identificador de Usuario a Individuos que están fuera de la Organización

No se proporcionaran identificadores de usuarios para el acceso a los sistemas de información Banco X. Aquellos individuos que no son empleados, contratista o consultores, a menos que exista la aprobación escrita del un vice-presidente y/o gerente de área responsable de las actividades del mismo.

85. Conciencia del Usuario sobre el Registro de Violaciones de Seguridad

Los usuarios deben estar debidamente informados sobre las acciones que constituyen infracciones de seguridad y que tales infracciones sean registradas.

86. Información Secreta en Computadores Portátiles

Los empleados que posean dispositivos portátiles, un laptop, un libro de anotaciones, agendas u otro dispositivos similar que contenga información confidencial del Banco X, no deben dejarlo desatendido a menos que la información esté cifrada.

87. Revocación de los Privilegios de Accesos a los Sistemas del Banco X.

La Gerencia de Seguridad de Datos, debe revocar los privilegios de accesos a los sistemas de información computarizados inmediatamente que un empleado deje de prestar servicio a la Institución.

88. Restricciones de Accesos no Autorizados en los Sistemas de Información Banco X.

La Gerencia de Seguridad de Datos del Banco X, debe vigilar la configuración adecuada de los sistemas de información computarizados del Banco X, afín de evitar que los empleados que utilizan los sistemas de información obtengan acceso no autorizado a los mismos, pudiendo afectar su funcionamiento normal y operatividad. Asimismo, se prohíbe a los empleados del Banco X capturar contraseñas, claves de encripción o evitar cualquier otro mecanismo de control de acceso implantado

2.02.06 Actividades Administrativas

89. Cambio Forzado de todas las Contraseñas

Siempre que la seguridad de un sistema haya sido comprometida, o exista conocimiento o sospecha de la vulnerabilidad de los mecanismos de control implantados en este, el (los) administrador(es) de seguridad, deben cambiar inmediatamente cada contraseña definida en el sistema. Igualmente, bajo cualquiera de estas circunstancias, deben ser revisados todos los privilegios de usuarios definidos en el sistema.

90. Revisión Periódica de las Asignaciones de Perfiles y Privilegios de Acceso

Los perfiles y privilegios de acceso definido en los sistemas de información y/o servicios de comunicación otorgados a los usuarios, deben ser re-evaluados periódicamente por la vice presidencidencias o gerencias involucradas, en base con las necesidades del negocio. Esta evaluación debe hacerse en coordinación con la Gerencia de Seguridad de Datos.

91. Requerimientos para la Emisión de Perfiles de Usuarios

Antes de ser asignado un perfil de usuario, los empleados deberán conocer las normativas de seguridad de Activos de Información de la Institución. En tal sentido, deben ser utilizados los medios necesarios para el conocimiento de tales normativas, firmando un acuerdo en señal de aceptación de las mismas al momento de iniciar la relación laboral.

92. Utilización de Estándares para los Recursos de las Diferentes Plataformas

A fin de facilitar la administración y mantenimiento de los recursos del Banco X y lograr un ambiente de control consistente se debe procurar la aplicación efectiva de una nomenclatura estándar para la definición y asignación de perfiles de usuarios, nombres de programas y archivos de producción, estaciones de trabajo, servidores y otros recursos.

93. Herramientas para Verificar el Estado de Seguridad de los Sistema Multi-Usuarios del Banco X.

Cada sistema de información computarizado del Banco X debería incluir herramientas automatización que permita al administrador verificar el estado de seguridad y corregir los problemas detectados. Asimismo, las configuraciones y parámetros de seguridad definidos en las plataformas operativas, deben obedecer las normativas de seguridad descritas en este documento.

94. Cambios de Privilegio de los Usuarios

Todos los cambios en las responsabilidades de los usuarios, así como las transferencias y terminaciones de empleo, deben ser comunicados a la brevedad posible a la Gerencia de Seguridad de Datos, a fin de que el administrador de Seguridad pueda realizar los cambios en el ambiente operativo de manera inmediata. En tal sentido, la Vice-presidencia del Área de Recursos Humanos debe participar en este proceso. La intención de esta política, es mantener actualizados los privilegios de accesos de los usuarios según sus funciones actuales.

2.02.07 Sistema de Correo Electrónico

95. Uso del Correo Electrónico

El sistema de correo electrónico es una herramienta de gran valor y ha sido establecida para ser utilizada con fines del negocio. En tal sentido, su uso no esta asociada a actividades personales, comerciales ni aquellas que coloquen al Banco X en una posición potencialmente riesgosa.

96. Privacidad del Correo Electrónico

Todos los mensajes de correo electrónico deben ser considerados como información privada. El correo electrónico debe ser manejado como una comunicación privada y directa entre un remitente y un destinatario, de igual forma que el correo tradicional.

97. Uso de la Cuenta de Correo Asignada a otra Persona

Los empleados no deben utilizar cuentas de correo electrónico asignada a otras personas para evitar o recibir mensajes. En caso de que se necesite leer correo de

otra persona (por encontrarse de vacaciones, por ejemplo) debe utilizarse el mecanismo de remisión de mensajes “forwarding” u otras facilidades similares. Adicionalmente, esta política interna de prevenir que los empleados hagan uso de cuentas de correo asignadas a otras personas, para simular al remitente.

98. Remisión de Correo Provisto por Fuentes Externas

Los empleados del Banco X no deben remitir mensajes enviados por terceros los cuales puedan considerarse no acordes a las prácticas del negocio, o que pudieran contribuir a crear un ambiente hostil en la Institución. Es de hacer notar, que un ambiente de trabajo hostil puede ser generado por comentarios denigrantes en relación con raza, religión, preferencias sexuales entre otros.

99. Registro y Retención de Correo Electrónicos

Los administradores del sistema de correo electrónico del Banco X, deben establecer y mantener los procesos sistemáticos para el almacenamiento (respaldo) retención y destrucción de correo electrónicos. Adicionalmente, los sistemas de correo deben estar configurados de tal manera que todos los mensajes recibidos y/o enviados queden debidamente registrados en un “log” que debe ser revisado y borrado con una frecuencia establecida. La destrucción tanto del “log” como los mensajes referenciados en éste, puede ser pospuesta en caso de que exista algún inconveniente asociado al manejo del correo electrónico, así como también en caso de que este material contenga información potencialmente importante y pudiera ser utilizado como evidencia en una acción legal por parte del Banco X, sobre un empleado.

100. Prohibición del Uso del Correo Electrónico como Repositorio de Información

Todos los empleados del Banco X, deben transferir la información considerada importante desde su buzón de correo electrónico a documentos almacenados en su entorno de trabajo, manejables por aplicaciones como procesadores de palabras, hojas de cálculo, bases de datos y otras; en caso que no tengan archivo anexos, convertirlos a un documento manejable por el sistema de correo electrónico del Banco X. La intención de esta política es concienciar a los usuarios de que las facilidades del correo electrónico no deben ser utilizadas como repositorio de información importante, ya que los mensajes pudieran:

a. Ser borrados accidentalmente por los usuarios

b. Dañarse en caso de fallas del sistema.

c. Ser eliminados por los administradores del sistema, tal como lo refiere la política anterior.

101. Envío de Información confidencial a través del Correo Electrónico

A menos que la información esté encriptada, los usuarios del correo electrónico deben abstenerse de enviar información confidencial tales como proyectos de negocios, estadísticas, estudios, estados financieros, así como información de seguridad tales como contraseña, cuentas de usuarios y otras.

102. Autorización para Leer los Correos Electrónicos Pertenecientes a Otros Empleados

A menos que estén explícitamente aprobado por el Gerente responsable, los empleados de Banco X, no deben leer correos que no le pertenezcan. Una excepción a esta política la constituye el seguimiento del flujo de correo electrónico en la institución, en donde la Gerencia del Área de Tecnología, la Gerencia de Seguridad de Datos y la Vice-presidencia de Recursos Humanos acuerden la revisión de los mensajes recibidos por los empleados, a fin de detectar complicidad interna, actividades sospechosas o cualquier otra razón administrativa.

103. Restricciones en el Contenido de los Mensajes

Todos los empleados del Banco X, deben evitar enviar o remitir mensajes con información potencialmente ofensiva y que puedan colocar a algunos individuos en una posición vergonzosa y hasta legalmente comprometedora. Por tal motivo, todas las comunicaciones emitidas y/o recibidas por correo electrónico, deben preservar la conducta ética y profesional que el remitente y/o destinatario debe mantener como miembro del Banco X. Por tal motivo, los siguientes aspectos están estrictamente prohibidos:

a. Transmisión de mensajes ilegales, de acoso o amenazantes.

b. Generación, transmisión o almacenamiento de información potencialmente ofensiva. Esta incluye, pero no está limitada a: bromas sobre color de piel, material denigrante de cualquier etnia, basada en géneros u otro grupo de personas, o material sexualmente explícito.

c. Acceder o descargar material de mensajes tipo postales de mal gusto.

d. Enviar materiales sensibles o confidenciales del Banco X o de un cliente a terceros.

e. Cualquier uso que resulte en beneficio personal.

f. Uso excesivo del correo electrónico o descarga de archivos para uso no profesional y que puedan congestionar el sistema de correo.

g. Quienquiera que reciba un mensaje inapropiado por correo electrónico o e-mail, debe notificar al Gerente responsable de su departamento o a la Vice-presidencia del Área de Recursos Humanos.

104. Transmisión de Correos en Forma Masiva

La transmisión de mensajes utilizando el correo electrónico en forma masiva, debe ser autorizador por la Gerencia responsable, en coordinación con la Gerencia del Área de Tecnología y tratarse únicamente de asuntos relacionados con la Institución, a fin de evitar el congestionamiento del sistema de correo electrónico. En tal sentido, los siguientes aspectos está estrictamente prohibido:

a. Generación o diseminación de cartas tipo cadena

b. Diseminación ampliada (difusión de mensajes) no relacionados al negocio

Dichos envíos deben cumplir con las siguientes características:

a. Tamaño ajustado de los Correos: Uno de los aspectos más importante dentro del mundo del correo electrónico es su tamaño. El mismo incide de manera directa en su tiempo de transmisión y en la posibilidad de recepción del mismo. Es importante destacar que muchas de las cuentas de correos son gratuitas y poseen limitaciones de capacidad, motivo por la cual un correo con un tamaño superior a 3 MB, posiblemente no sean recibidos por una cuenta gratuita. En tal sentido se recomienda que los mismos al momento de ser construidos sean inferior a 200 K en formato HTML y con imágenes referenciadas en vez de adjuntadas.

b. Envío en forma controlada: Fraccionar el envío masivo de correos en lotes. Lotes que no deben contener más de 10.000 direcciones. Cuando existan más de unos lotes, cada lote debe ser enviado con un intervalo de una a dos horas entre ellos. En la medida posible, el envío de estos correos deben hacerse durante el horario no laboral y preferiblemente los días viernes.

c. Destinatarios Certificados: Las direcciones de correo de los destinatarios seleccionados deben ser lo más fiel y certera posible para evitar comportamiento errático del servicio.

105. Revisión de los Volúmenes del Servidor de Correo Electrónico

La Gerencia del Área de Tecnología, específicamente del Departamento de Comunicaciones la cual es responsable del sistema de correo electrónico, deben

establecer la frecuencia de revisión de los volúmenes del servidor donde residen los buzones de correos electrónicos, a fin de identificar el uso inadecuado de este sistema. En tal sentido, la Gerencia del Área de Tecnología se reserva el derecho de programar de forma automática la revisión y filtrado del tamaño de los mensajes de correo, y en caso de que un correo sea rechazado por el tamaño del mismo, se le notificará al usuario involucrado y se tomarán las acciones pertinentes.

106. Los Mensajes de Correo Electrónico como Información del Banco X.

Los empleados del Banco X deben entender que todos los mensajes enviados por correo electrónico, tanto externa como internamente es información propiedad del Banco X. Por tal motivo, la Institución se reserva el derecho de acceder y revisar los mensajes enviados por este sistema para cualquier propósito, bien sea para determinar si existen brechas de seguridad, si se ha violado alguna política del Banco X, o se han tomado acciones no autorizadas. Asimismo, la revisión de los correos electrónicos enviados por los empleados del Banco X, puede ser requerida por razones de tipo legal, sin previa notificación a los empleados involucrados.

107. Acceso al Sistema de Correo Electrónico

Todos los empleados del Banco X deben utilizar una cuenta de usuario y una contraseña para el acceso al sistema de correo electrónico, cumpliendo con las normativas de administración del identificador de usuario y contraseñas. Al ausentarse de la oficina, los empleados deben cerrar el sistema de correo electrónico o utilizar el protector de pantalla con contraseña como medida de protección.

108. Envío / Recepción de Información por Correo Electrónico

El correo electrónico es una herramienta de gran valor y su uso es importante para el Banco X. Al mismo tiempo, el correo electrónico representa un medio potencial para la propagación de virus y otros programas mal intencionados. En tal sentido, cuando se envíe y/o reciban archivos de datos, documentos, etc., deben asegurarse que los mismo no contengan virus que puedan afectar el funcionamiento normal del sistema.

Manejo de Equipos de Computación

109. Expansión y Alteración de Equipos de Computación del Banco X.

La Gerencia del Área de Tecnología será responsable de alterar en la configuración de los equipos de computación perteneciente al Banco X (estaciones

de trabajo, computadoras portátiles, impresoras, servidores de impresión, etc.) En tal sentido, en caso de que se requiera alguna alteración en un equipo, la misma debe canalizarse con la Gerencia del Área de Tecnología mediante una solicitud formal. Las referidas alteraciones incluyen: expansión de memoria, actualización del procesador, inserción o extracción de circuitos electrónicos, entre otros.

110. Protección de la Información del Banco X en Trabajo Fuera de Oficina

Los empleados que estén autorizados a realizar trabajos fuera de la oficina, deben tomar las precauciones necesarias para proteger de forma razonable el hardware, software o cualquier otra información que le haya sido asignado contra robo, pérdidas y daños

111. Reporte de Pérdidas o Daños de Hardware / Software

Los empleados del Banco X deben reporte cualquier robo o daño ocurrido en su equipo de trabajo o información que le haya sido confiada para su uso y cuidado a la brevedad posible a la Gerencia encargada del área en el cual trabaja o al supervisor inmediato, quien debe notificar a su vez a la Gerencia del Área de Tecnología y a la Gerencia de Seguridad de Datos. Esto permitirá tomar las acciones pertinentes de manera oportuna.

112. Política de Seguridad de Activos de Información para Comunicaciones Remota

Como una condición para conceder el derecho de acceso remoto para trabajar fuera de oficina, el empleado debe estar en conocimiento y de acuerdo con las políticas de seguridad de activos de información establecidas por el Banco X. Estos incluyen pero no se limita a acuerdo de manejo de licencias legales, uso de información autorizada y otros.

113. Uso de Computadora Personales Propiedad de los Empleados o Terceros

Los empleados del Banco X no deben traer sus propias computadoras, periféricos o programas a las instalaciones de la Institución. Cuando se trate de contratistas o terceros, la función de la Gerencia del Seguridad de Datos y la Gerencia del Área de Tecnología, deben estar en conocimiento del uso de computadoras personales a fin de establecer los controles necesarios. Las excepciones a estas políticas serán manejadas por el Área de Seguridad de Datos.

2.02.08 Respaldo, Almacenamiento y Recuperación de Información

114. Frecuencia de Respaldo e Información a respaldar

Todas la información sensible, valiosa o crítica que resida en los sistemas de computación del Banco X (aplicaciones, software base, datos, etc.) debe ser respaldada al finalizar la jornada de trabajo, de acuerdo a su clasificación, a los requerimientos del negocio o cuando se efectúen modificaciones a los sistemas, a fin de poder realizar cualquier recuperación que sea necesaria después de una contingencia. Adicionalmente, la información vital debe ser almacenada en un sitio protegido desde el punto de vista físico, con control de acceso y debe estar incluida en los planes de contingencia, para que dichos respaldo puedan ser utilizados en caso de emergencia.

115. Respaldo de Información en Computadora Portátiles.

Todos los empleados del Banco X a quien se les haya asignado una computadora portátil para realizar trabajo fuera de oficina, deben realizar respaldo periódico locales de la información de interés para el webmaster, a fin de evitar pérdidas considerables en caso de robo a daño del equipo portátil. La Gerencia del Área de Tecnología debe proveer los recursos e indicaciones necesarias para que los empleados realicen sus respaldos de manera exitosa.

116. Uso de los Servicio de una Bóveda Externa

A fin de mitigar los efectos de un desastre y para facilitar la recuperación de la información ante la ocurrencia de una contingencia que afecte las instalaciones del Banco X, se debe contar con los servicios de una bóveda externa donde se envíe al menos dos (2) veces por semana, un juego del respaldo de la información del webmaster. En tal sentido, la Gerencia del Área de Seguridad de Datos debe realizar la planificación y coordinación necesaria con el ente externo a utilizar, y establecer aspectos tales como el personal responsable del resguardo de la información, periodicidad de envío y otros.

117. Notificación a los Empleados en Caso de Respaldos Totales o Recuperación Especiales

En caso de que por alguna actividad extraordinaria se requiera hacer respaldos totales o recuperación de la información y se requiera que no se esté utilizando el sistema, la Gerencia del Área de Tecnología debe notificar con anticipación a todos los empleados la realidad de dicha actividad, a fin de que no se entorpezca el proceso o recuperación.

118. Precaución en el Uso de la Información Respaldada en el Proceso de Recuperación

Antes de utilizar la información respaldada en un proceso de restauración, se deben tomar las precauciones necesarias para evitar que la única copia de respaldo se dañe inadvertidamente durante el proceso de restauración.

119. Período de Retención de la Información

Toda la información de contabilidad fiscal y de naturaleza legal del Banco X, debe ser resguardada en forma segura durante un período no menor de cinco (5) años. Todos los demás registros deben ser retenidos durante el período que se establezca basándose en las necesidades de la organización. Los documentos resultados de las negociaciones financieras, negociaciones, etc. y los archivos de entrada electrónica originales deben ser retenidos hasta que hayan sucedidos tres eventos específicos:

a. Las operaciones contempladas hayan concluido.

b. Los registros de ingreso de estas operaciones hayan sido revisados por el gerente del área.

c. Toda la información que deje de ser necesaria, debe ser destruida, previa evaluación del propietario de la información en actividad conjunta con el personal responsable de la Gerencia de Seguridad de Datos.

120. Realización de Pruebas Periódicas de la Información Respaldada

Toda la información del negocio que ha sido respaldada en medio de computación durante período de tiempos prolongados, deberá ser sometida a pruebas periódicas, para asegurar que la misma es recuperable. En tal sentido la Gerencia de Seguridad de Datos, en actividad conjunta con la Gerencia del Área de Tecnología, deberá dirigir las pruebas periódicas.

2.02.09 Acceso a la Internet

121. El Acceso a Internet Acorde con las Funciones

Los privilegios de acceso a la Internet están reservados para aquellos empleados que lo requieran según sus funciones de trabajo y de acuerdo a las necesidades del negocio. Todo acceso a la Internet por parte de los empleados del Banco X debe ser aprobado previamente por la Gerencia correspondiente, la Gerencia del Área de Tecnología y la Gerencia de Área de Seguridad de Datos. Asimismo, debe proporcionarse un adiestramiento sobre las normas de uso seguro de Internet a fin de evitar el uso irrestricto de los empleados de la Institución.

122. Registro de Acceso a Internet

Todas las conexiones y acceso deben quedar debidamente registrados y los Logs de accesos deben ser revisados por el Departamento de Comunicaciones en concordancia con las políticas establecidas en este documento, la cual se realizaría con una frecuencia específica, a fin de detectar de manera pro activa accesos o intentos de accesos no autorizados a la ejecución de funciones dañinas que pudieran comprometer la operatividad de la red del Banco.

123. Administración de Cuentas con Acceso a Internet

El acceso a Internet debe estar asociado al identificador de usuario de red y regulado por los mismos lineamentos de administración de perfiles de usuarios y contraseñas locales del Banco X. La renovación de las contraseñas se regirán por las políticas de cuentas en la red interna.

124. Autenticación Extendida para Usuarios Externo al Banco X.

Todo usuario que desee establecer conexión con la red del Banco X vía Internet, debe ser autenticado antes un firewall antes de obtener el acceso a la red interna de la Institución. El uso de sistema de autenticación extendida permitirá prevenir que usuarios no autorizados pueden hacer uso de contraseñas fijas las cuales eventualmente pueden ser capturadas vía Internet.

125. Envío de Mensajes Personales Vía Internet

Siempre que un empleado utilice las facilidades de Internet (correo, foros de discusión o cualquier otro sistema de información pública) para el envío de mensajes personales, los mismos no deben proveer información sobre proyectos, productos o planes del Banco X que puedan causar impacto en el negocio. Se hará excepciones en caso de que el origen de los mensajes sea de algún ente interno autorizado explícitamente por el Banco X.

126. Divulgación de los Productos y Servicios Prestados por el Banco X.

Los empleados no deben divulgar, promover, presentar o hacer declaraciones sobre productos y servicios ofrecidos por el Banco X en foros de Internet, tales como listas de correo (mailling list) “new group” ó sesiones de “chat” sin la previa aprobación de las Unidades de Negocios involucradas. Esta políticas intenta controlar la divulgación sobre los productos y servicios que ofrece el Banco X.

127. Derecho de Autor (propiedad intelectual) en Internet

A pesar de que Internet es un medio de comunicación informal, aún aplican las leyes de derechos de propiedad literaria, patente, marcas de fabricación y similares. A tal efecto, los empleados de Banco X que utilicen Internet deben:

a. Adquirir la información de Internet sólo después de obtener permiso de la fuente, en caso de que sea necesario.

b. Citar la información obtenida de Internet, siempre y cuando las fuentes estén identificadas.

c. La información pública del Banco X será mostrada en Internet, sólo si la misma ha sido oficialmente aprobada para su liberación pública y se ajusta a la clasificación de la información.

128. Declaración de Políticas Legales y Transferencia de Productos y/o servicios

Los empleados del Banco X con acceso a Internet deben abstenerse de hacer cualquier declaración legal o endoso de productos y/o servicios que pueda comprometer la imagen del Banco X, a menos que sea previamente autorizado por la(s) gerencia(s) involucrada(s).

129. Participio en Grupo de Discusión en Internet

La participación del Banco X en grupo de discusión y otros foros públicos de Internet relacionados al sector bancario, debe estar restringida a empleados designados para tal fin, a los cuales se les hayan establecido la información del negocio que puede ser revelada ante terceros. Asimismo, dicha participación debe armonizar con las prácticas del negocio y en todo momento, se prohíbe el uso de vocabulario que pueda afectar la imagen de Banco X, como por ejemplo: lenguaje inadecuado, discriminación religiosa, raciales, de edad, sexo y similares.

130. Las Páginas Web extra-oficial será sólo permitidas por Contrato

No debe publicarse páginas web-extra oficiales, que anuncie productos y/o servicios por el Banco X, a menos que esté especificado en el contrato que regula la prestación de “hosting” por parte d terceros o que haya sido autorizado previamente por el Banco X.

131. Publicación de Información en la Página Web del Banco X.

Ningún empleado del Banco X debe colocar información relacionada a la Institución (software, memos internos, informes, estadísticas, etc.) en la página web del Banco X. Por el contrario, sólo el “webmaster” (diseñador) de la

compañía proveedora de servicio de Internet o del Banco X, serán los responsables de esta función, previo acuerdo con las gerencias involucradas.

132. Administración de Cambios en la Página del Banco X.

Cualquier cambio de página del Banco X, debe cumplir con los lineamientos por el área responsable del diseño de la página antes de ser publicado. Esta área se asegurará que todas la información publicada ha sido evaluada en función de apariencia, es consistente con las metas estratégicas del negocio y si reúne las medidas de seguridad adecuadas.

133. Requerimiento de Diseño de la Página Web del Banco X.

Todas las páginas web del Banco X deben cumplir los estándares de diseño establecidos por la Institución con el proveedor del servicio de diseño, así como estándares de navegación, normas legales de redacción y requisitos similares aprobados por la Vice-presidencia de Negocios.

134. Aprobación de Uso de Enlaces Directos con Otras Entidades

El uso de enlace directo “hot-links” los cuales transfieren las sesiones de usuarios de “web site” del Banco X a otra entidad (enlace saliente) y viceversa (enlaces entrantes) deben ser autorizados por la Vice-presidencia de Administración y Tecnología.

135. Envío de Información de Seguridad por Internet

Los empleados del Banco X no deben enviar contraseña o cualquier otra información de seguridad manejada internamente por correo electrónico o cualquier otro servicio de Internet, si dicha información puede ser leída por cualquier persona que intercepte el mensaje.

136. Envío de Software o cualquier otra Información Confidencial por Internet

Toda información confidencial que sea propiedad del Banco X no debe ser enviada por Internet, a menos que se tomen medidas de protección que garantice su integridad y confidencialidad, generalmente bajo el enfoque de encripción basado en los mecanismos seleccionados para tal fin.

137. Encripción de Archivo de Servidores FTP Anónimos

Toda la información provista por servidores FTP anónimos del Banco X, debe estar encriptadas de acuerdo al mecanismo seleccionado para tal fin. Esta política no es aplicable en caso de que se trate de información liberada para el uso público seleccionado para tal fin. Esta política no es aplicable, en caso de que se trate de información liberada para el uso público.

138. Manejo de Software y Archivos Provenientes de Internet

Todos el software y archivo que sean obtenidos desde Internet u otra red pública, deben ser revisados con el uso de software anti-virus antes de que sean utilizados por otras aplicaciones, tales como procesadores de palabras, hojas de cálculos, graficadores o similares, a fin de reducir el riesgo de propagación de virus en la red de Banco X, reduciendo de esta manera los daños y problemas relacionados.

139. Confiabilidad de la Identidad de Grupo Externo Dentro de Internet

En redes públicas como Internet es relativamente fácil falsificar la identificación de otro. El uso y/o acceso remoto a las redes y/o sistemas del Banco X, debe ser concedido sólo por razones de negocio. En tal sentido, se deben implementar mecanismos de control de acceso remoto en el firewall que garanticen la identificación y autenticación del usuario antes de aceptar la conexión a la red y/o a los sistemas del Banco X.

140. Intercambio de Información Vía Internet

Todo intercambio de software y/o cualquier otra información entre el Banco X y terceras partes, debe ser autorizado por la(s) gerencia(s) involucrada(s) y coordinadas con la Gerencia del Área de Seguridad de Datos y la Gerencia del Área de Tecnología, especificando los términos de intercambio, así como las maneras de cómo el software y los datos serán manejados y protegidos.

141. Uso de Software Provenientes de Internet

Los empleados del Banco X no deben utilizar software proveniente de terceros obtenidos del Internet en ninguna computadora perteneciente al Banco X, a menos que haya sido autorizado previamente por la Gerencia del Área de Tecnología y la Gerencia de Seguridad de Datos.

142. Control de la Información Obtenida por los Usuarios en los Sitios Web de Internet

Siempre que se obtenga información vía Internet, los usuarios deben verificar las condiciones de dicha información para poder ser utilizada y no provocar una influencia negativa para la Organización.

143. Establecimiento de Negocios Vía Internet

Los empleados del Banco X no podrán establecer negocios ni acuerdos comerciales con terceros utilizando las facilidades de la Internet de la Institución. En caso de que los acuerdos comerciales estén relacionados a cualquier área, los

mismos deben ser autorizaos por la gerencia involucrada. La intención de esta política es detener iniciativas de hacer negocios personales en cualquier área.

144. Desactivación de Leguaje JAVA en los Navegadores (browsers)

Todos los empleados del Banco X que utilicen las facilidades de Internet, debe tener configurado la desactivación de la ejecución de programa JAVA o alguna otra herramienta similar de forma tal que se restrinja las capacidades de acceso o uso, modificación y eliminación de activos de información. Esta configuración puede ser diferente sólo en los casos en que los usuarios visitan web-site confiables.

145. Control de Ejecución de Aplicaciones en JAVA

Sólo debe permitirse a los empleados del Banco X que utilicen las facilidades de Internet, la ejecución de aplicaciones en JAVA “applets” cuando:

a. Provenga de una fuente confiable

b. La firma digital haya sido verificada.

El derecho de ejecutar sobre aplicaciones en JAVA, puede ser una fuente potencial de inserción de virus, “Caballos de Troya” o cualquier otro código de programa que atente sobre la integridad de la información de los equipos del Banco X. Esta política asume una audiencia de usuarios técnicamente consciente de los riesgos que la violación de esta política pudiera ocasionar.

2.03. Desarrollo de Sistema y Control de Cambios

2.03.01 Análisis de Especificaciones de los Requerimientos de Seguridad

146. Identificación de Requisitos de Seguridad

Antes de desarrollo o adquirir un nuevo sistema, la gerencia del departamento usuario debe haber especificado claramente los requisitos relevantes de seguridad.

147. Inclusión de Seguridad en Sistemas

Los desarrolladores de sistemas internos deben incrustar la seguridad dentro de los sistemas que construyan o mejorar todas las instalaciones en las que haya una solución disponible comercialmente, a costo razonable y generalmente aceptada.

148. Especificaciones para Software Desarrollo Internamente

Todo software desarrollado por personal interno que se utilice para procesar información sensible, valiosa o crítica debe poseer una especificación formal por escrito que forme parte de un acuerdo entre el propietario de la información y el

desarrollador del sistema, redactada y elaborada antes de que comience los esfuerzos de programación

149. Principios de Codificación de Aplicación

Deben utilizarse principios y prácticas seguras de codificación, especificados y actualizados por la Gerencia de Seguridad de Datos para todo el software desarrollado o mantenido internamente.

150. Seguridad en el Ciclo de Vida del Desarrollo de los Sistema

Para todos los sistemas de aplicaciones de negocios, los diseños y desarrolladores de sistemas deben considerar la seguridad desde el principio del proceso de diseño de los sistemas, hasta su conversión en sistemas de producción.

151. Fallas de Operación de software

Cada vez que le software desarrollado internamente falle y no produzca los resultados esperados, siempre debe proporcionar un mensaje de error o alguna otra indicación de falla como respuesta al operador.

3.Seguridad Física Ambiental

3.01 Áreas Seguras

152. Solidez de las Puertas del Centro de Computación

Los salones de los centros de computación deben estar equipados con puertas antimotines, puertas resistentes al fuego y cualquier otra puerta resistente a entradas forzadas

153. Puertas Adicionales de Acceso al Centro de Computación

Todas las puertas adicionales de un centro de computación deben estar equipadas con barras de choque que activen una alarma al abrirse.

154. Control de Acceso a la Áreas donde Reside la Información del Banco X.

El acceso al área de trabajo donde se maneja la información importante del Banco X debe estar restringido físicamente. En tal sentido, debe estar establecidas medidas de seguridad más efectivas para garantizar el acceso a dichas áreas y esté restringida a personas autorizadas.

155. Control de Acceso a la Salas de Servidores y Equipos de Comunicación y Telefonía

Todos los equipos de comunicación, telefonía y servidores del Banco X deben estar ubicados en áreas de accesos restringidos, a fin de evitar cualquier entorpecimiento de dichos sistemas a causas de actividades accidentales o

intencionales contra los equipos. Asimismo se limitará el acceso sólo para aquellas personas cuyas funciones así lo requieran, o a las personas debidamente autorizadas por la Gerencia del Área de tecnología.

156. Permanencia de las Puertas Abiertas del Centro de Cómputos

Siempre que las puertas del Centro de Cómputos permanezcan abiertas por razones de mudanzas de máquinas, mobiliarios, suministro o cualquier otro producto similar, la entrada debe ser continuamente monitoreada por cualquier persona de la Gerencia del Área de Tecnología, en conocimiento del responsable de la Gerencia de Seguridad de Datos.

157. Prohibición de Realización de Trabajo dentro del Centro de Cómputo.

Ningún usuario, cuyo trabajo no esté directamente asociado con el Centro de Cómputo, telecomunicación etc., podrá realizar trabajo en estas áreas.

158. Fumar, Comer y Beber

Los trabajadores y visitantes deben abstenerse de fumar, comer y beber en el área del Centro de Cómputo.

159. Controles Ambientales del Centro de Computación.

La Gerencia local debe suministrar y mantener adecuadamente los sistemas de prevención y supresión de incendio, aires acondicionados, control de humedad y otros sistemas de protección de ambientes computarizados, en todos los centros de computación del Banco X.

160. Alarmas del Centro de Cómputo

El Centro de Cómputo del Banco X debe estar equipado con sistemas de alarmas contra incendios, agua e intrusión física que automáticamente alerten a aquellos en capacidad de tomar medidas inmediatas.

161. Seguridad Física de la Información

Toda la información que se encuentre en medio electrónico, tales como: cintas, CD-ROOM y otros que deban ser almacenadas fuera del Centro de Cómputo, debe ser resguardada bajo llave cuando la misma no esté en uso. Una excepción se hará si la información es protegida vía un sistema de encripción aprobada por la Gerencia de Seguridad de Datos.

162. Pase de Autorización para la Salida de Equipos de Computación y Telecomunicación No podrán producirse salidas de equipos de computación y telecomunicación, tales como: computadoras portátiles, MODEMS, radios portátiles o similares, sin la debida autorización de los líderes del área vinculadas

a la Gerencia del Área de Tecnología. Esta autorización debe ser materializada a través de un pase de salida, el cual debe contener la firma de la persona que autoriza la salida del equipo.

163. Entradas y Salidas de Materiales la Centro de Cómputo

Debe existir personal encargada de las salidas y entradas de materiales del Centro de Cómputo. El personal que realice la entrega o que necesita retirar algún material del centro de cómputo, no debe tener acceso a esta área.

3.02. Registro de Acceso a las Salas de Máquinas

164. Acceso de Terceros al Centro de Cómputo.

El acceso de personas externa al Banco X (clientes, ex empleados, familiares de trabajadores, contratistas, personal de reparación de equipos y/o cualquier otro visitante) debe ser permitido sólo si existe un empleado autorizado por la Gerencia del Área de Tecnología como acompañante y en horas laborales. En ningún caso podrá permitirse el libre acceso a personas externas del Banco X al Centro de Cómputo.

165. Acceso al Centro de Computación

Los programadores, los usuarios y otros que no tengan necesidad de negocio para tal acceso, no deben entrar a los centros de computación.

166. Acceso del Personal al Centro de Computación

El Gerente o Jefe de operaciones debe mantener una lista revisada y actualizada por lo menos cada tres meses, del personal con acceso al centro de computación.