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

Trabajo de Grado de Maestría

MODELO DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN PARA EL MONITOREO Y ANÁLISIS DEL TRÁFICO DE REDES EN LA ADMINISTRACIÓN PÚBLICA NACIONAL DE VENEZUELA.

Presentado por:
Vargas Piñango Ángel Pastor
Para optar al Título de
Magíster en Sistema de Información

Tutor
Dr. Bonillo, Pedro

Caracas, Junio 2016

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

Trabajo de Grado de Maestría

MODELO DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN PARA EL MONITOREO Y ANÁLISIS DEL TRÁFICO DE REDES EN LA ADMINISTRACIÓN PÚBLICA NACIONAL DE VENEZUELA.

Presentado por:
Vargas Piñango Ángel Pastor
Para optar al Título de
Magíster en Sistema de Información

Tutor
Dr. Bonillo, Pedro

Caracas, Junio 2016

Universidad Católica Andrés Bello
Dirección General de los Estudios de Postgrado
Postgrado Sistemas de Información
Ciudad.-

Referencia: **Aprobación de Tutor**

Tengo a bien dirigirme a Usted a fin de informarle que he leído y revisado el borrador final del Trabajo de Grado titulado "MODELO DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN PARA EL MONITOREO Y ANÁLISIS DEL TRÁFICO DE REDES EN LA ADMINISTRACIÓN PÚBLICA DE VENEZUELA". Presentado por el Lic. Vargas Piñango Ángel Pastor, titular de la cédula de identidad N° 10.867.159, como parte de los requisitos para optar al Título de Magíster en Sistema de Información.

A partir de dicha revisión, considero que el mencionado Trabajo de Grado reúne los requisitos y méritos suficientes para ser sometido a evaluación por los distinguidos Jurados que tenga(n) a bien designar.

Atentamente,

Bonillo Pedro

Dr. Pedro Bonillo
C.I. 10.868.538

DEDICATORIA

A mis padres, que aun no estando físicamente, si están en todas las cosas que hago y los llevo siempre presente.

A mi esposa Jacqueline Valencia, que siempre ha estado conmigo en todo momento. Te amo.

A mis hijos, Julio Cesar y Cesar Augusto, que son mi principal motivación para seguir luchando.

A mis hermanos, que son motivo de alegría y que forman parte de las cosas buenas de mi vida

AGRADECIMIENTOS

A mi esposa Jacqueline, que siempre me ha animado a seguir adelante, en todo momento.

A mi profesora María Esther, que siempre me estuvo motivando a culminar el proyecto y alcanzar la meta.

A mis compañeros del IVSS que me ayudaron y me prestaron el apoyo para lograr los objetivos planteados.

A todos, un millón de gracias

ÍNDICE GENERAL

Índice de tablas

Índice de Figuras

LISTADO DE ACRÓNIMOS

APN Administración Pública Nacional

AV Antivirus

BCP Plan de Continuidad de Negocios

BPIF Marco de Interoperabilidad de Procesos de Negocios

CDC Comités de Controles de Cambios

CGDN/DCSI Dirección Central de la Seguridad de los Sistemas de Información del Gobierno Francés

CIA Confidencialidad Integridad Disponibilidad

CMMI Integración de Modelos de Madurez de Capacidades

CNTI Centro Nacional de Tecnologías de Información

COBIT Objetivos de Control para la Información y Tecnologías Relacionadas

CRBV Constitución de la República Bolivariana de Venezuela

CSB Centro Simón Bolívar

DGI Dirección General de Informática

DNS Sistema de Nombres de Dominios

DOFA Debilidades Oportunidades Fortalezas Amenazas

DoS Denegación de Servicios

DRP Plan de Recuperación de Desastres

DSI Dirección de Seguridad de la Información

HTTP Protocolo de Transferencia de Hipertexto

IDS SIstema de Detección de Intrusos

IP Protocolos de Internet

ISO Organización Internacional de Nacionalización

ISO/IEC Organización Internacional de Normalización /Comisión Internacional de Electrotecnia

ISP Proveedor de Servicios de Internet

ISP Proveedor de Servicios de Internet

ITIL Librerías de Infraestructura de Tecnologías de Información

IVSS Instituto Venezolano de los Seguros Sociales

LDAP Protocolo Ligero/Simplificado de Acceso a Datos

LOAC Ley Orgánica de Administración Central

LOAP Ley Orgánica de Administración Pública

LOAP Ley Orgánica de Administración Pública

LSTA Ley de Simplificación de Trámites Administrativos

MMAGSI Modelo de Madurez Organizacional con Respecto a la Seguridad de la Información

MMS Modelo de Madurez de la Seguridad

OSI Interconexión de Sistemas Abiertos

PDF Formato de Documento Portátil

PISI Plan Integral de Seguridad Informática

PMMM Modelo de Madurez de Gerencia de Proyectos

PSC Proveedores de Servicios de Certificación

PyMES Pequeñas y Medianas Empresas

RAE Real Academia Española

RFC Petición de Comentarios

RTBD Base de Datos de Gestión de Requerimientos

SEI Instituto de Ingeniería del Software

SGDB Sistema de Gestión de Bases de Datos

SGSI Sistema de Gestión de la Seguridad Informática

SMTP Protocolo para Transferencia Simple de Correos

SQL Lenguaje Estructurado de Consultas

SUSCERTE Superintendencia de Servicios de Certificación Electrónica

TCP/IP Protocolo de Control de Transmisiones / Protocolos de Internet

TI Tecnologías de Información

TIC Tecnologías de Información y Comunicación

UPEL Universidad Pedagógica Experimental Libertador

USI Unidad de Seguridad Informática

VenCERT Sistema Nacional de Gestión de Incidentes Telemáticos

VPN Redes Privadas Virtuales

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERECTORADO ACADÉMICO
ESTUDIO DE POSTGRADO
ÁREA DE INGENIERÍA

MODELO DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN PARA EL MONITOREO Y ANÁLISIS DEL TRÁFICO DE REDES EN LA ADMINISTRACIÓN PÚBLICA DE VENEZUELA.

Autor: Ángel Vargas
Tutor: Pedro Bonillo
Fecha: Enero 2016

RESUMEN

El presente estudio tiene como objetivo proponer un modelo de madurez de Seguridad de la Información para el monitoreo y análisis del tráfico de redes en la Administración Pública Nacional en Venezuela, con el fin de establecer mecanismos que ayuden a centralizar el monitoreo proactivo de las redes institucionales que conforman los entes de la administración pública central, contra las amenazas que se presentan a diario en el contexto tecnológico. La Metodología aplicada es una investigación de campo de carácter exploratorio. El trabajo fue validado por el juicio de expertos. Por otra parte , se diseñó un instrumento de medición con la finalidad de determinar el nivel de madurez de la institución en materia de Seguridad de la Información.
Cabe destacar que se obtuvo un diagnóstico del estado actual de la Seguridad de la Información, como resultado del estudio realizado.
Se pudo concluir que aun cuando se cuenta con soluciones de hardware y software para minimizar las vulnerabilidades de seguridad presentes en la plataforma, la gestión de la seguridad tiene debilidades. Se recomienda dar a conocer a los involucrados que el mejoramiento de los procesos de seguridad informática no son finitos y por ende deben ser continuos.
Linea de investigación: Ingeniería del Software, Seguridad de la Información.

Descriptores: Sistemas de información, Modelo conceptual, Modelo de madurez, Seguridad de la información, Administración Pública Nacional.

INTRODUCCIÓN

El advenimiento de nuevas tecnologías ha generado el nacimiento de ámbitos de investigación que hace una década ni se pensaba tendrían tanto auge. El crecimiento en las telecomunicaciones, de la mano de la informática ha traído consigo grandes avances tecnológicos, que sin duda han devenido en cambios muy importantes e influido en el nivel de vida de todos. En medio de este crecimiento, el desarrollo de aplicaciones cada vez más especializadas y orientadas a satisfacer necesidades muy específicas ha permitido que la industria del desarrollo de aplicaciones tenga especial relevancia en nuestro días.

En décadas anteriores era común que el software fuese un añadido que los grandes comercializadores de equipos de computación suministraban a sus clientes para que pudieran tener utilidad.

Las necesidades particulares de cada quien fue lo que impulsó el desarrollo de las aplicaciones que cumplieran tareas que de otro modo serían particularmente tediosas, los programadores compartían sus aplicaciones y de este modo todos podían hacer uso de los programas sin mayores restricciones.

Sin embargo, las grandes corporaciones comenzaron a imponer restricciones a los usuarios de las aplicaciones y se comenzó a masificar el uso de

acuerdos de licencia, esto trajo como consecuencia que la libertad inicial de usar los programas y distribuirlos terminó.

A la par que el desarrollo de aplicaciones crecía, las redes informáticas que permitían conectar entre sí a computadores distantes uno del otro, bien sea en un edificio o en el área metropolitana de una ciudad o entre ciudades distantes entre sí.

Las tecnologías de interconectividad de redes, comenzaron a desarrollarse permitiendo que el uso de computadores que inicialmente se concibieron como herramientas de trabajo individuales, pronto comenzaron a ser parte de redes corporativas cada vez más grandes y llegando a la actualidad, donde un computador que no este conectado a una red ve reducidas significativamente sus posibilidades de uso.

A la par que se comenzaron a tener redes cada vez más complejas, el desarrollo de la internet, como la gran red de redes, ha permitido que la instantaneidad de la transmisión de la información nos permita estar al día con la información que precisamos en nuestro mundo actual.

Ya al comienzo del desarrollo de las primeras redes, los problemas inherentes a garantizar que la información que se compartía en dichas redes , tuviera el destino y uso que se suponía debían tener, hizo cada vez más necesario el desarrollo de tecnologías que garantizaran la seguridad de esa información.

El desarrollo de la seguridad informática, ha tenido especial auge aun desde los comienzos de las redes telemáticas, cada vez mas extensas. Los piratas informáticos irrumpen rutinariamente en entornos empresariales, militares, bancas virtuales, gubernamentales y otros entornos conectados en red.

A medida que los sistemas se vuelven generalmente más seguros, los métodos utilizados por estos atacantes se hacen más avanzados, involucrando la reposición intrincada, ingeniería social, compromiso físico y el uso de aplicativos específicos para atacar componentes periféricos de software, como antivirus o soluciones para realizar copias de seguridad que estén ampliamente desplegados dentro de redes corporativas.

De igual manera, podría esperarse que personal especializado en el área de seguridad de la información estén haciendo pruebas para tratar de solventar los problemas que representan este tipo de ataques a las redes de los ambientes empresariales.

En muchos de los casos, esto no resulta ser así, hay en la actualidad entornos operativos de empresas de diversos tamaños que presentan vulnerabilidades en la manera en que sus redes interactúan con redes externas.

La evaluación del estado de las redes actualmente operativas en las instituciones públicas, las potenciales vulnerabilidades que presenten y el desarrollo de un modelo de seguridad de la información, que a través del

monitoreo pro activo de las redes, y el establecimiento de métricas que permitan adelantarse a potenciales ataques la red. Todo esto con el objetivo de lograr un entorno informático de seguridad que procure mitigar los riesgos inherentes a dichas falencias.

En la elaboración del presente documento se ha buscado que las siguientes premisas se cumplan: que se mantenga la pertinencia del caso, se refleja la situación actual a nivel de la Administración Pública Nacional, se redacta de una forma accesible a la mayor cantidad de personas posible, se sustente en documentación actual y verificable, se presenten ventajas y desventajas del uso de la plataforma de seguridad informática propuesta y se mantenga una visión global del tema.

En resumen, este trabajo consta de seis capítulos, los cuales se organizan de la siguiente manera:

En el Capítulo I, se presenta la descripción, conceptualización, así mismo se detallan el objetivo general y los objetivos específicos de la investigación. Finalmente en este capítulo se tienen la justificación, el alcance y las limitaciones encontradas.

El Capítulo II, contiene los antecedentes más resaltantes y su relación con la investigación, posteriormente los fundamentos teóricos de la investigación, los cuales sirven de base para garantizar la estrecha relación entre el

proyecto y la teoría, bases contextuales, bases conceptuales y bases legales.

En el Capítulo III, se indica por medio del marco metodológico el tipo y diseño de la investigación, las técnicas y herramientas utilizadas para el desarrollo del proyecto, determinando todos los procedimientos y pasos necesarios para el levantamiento de información, el proceso de selección de la población y muestra, así como también los cuadros de identificación, y definición de las variables.

El Capítulo IV tiene como objetivo mostrar los resultados obtenidos de la aplicación de los instrumentos diseñados para elaborar el Modelo de Madurez, el Capítulo V presenta las conclusiones y recomendaciones y finalmente el Capítulo VI muestra una propuesta de Plan de Seguridad Informática orientado a posicionar a la Institución en el Nivel de Madurez idóneo para garantizar los niveles de seguridad.

Finalmente se tienen las Referencias bibliográficas y los anexos que complementan la información del trabajo de investigación, donde se pueden visualizar los instrumentos diseñados para la investigación y los resultados obtenidos de las respuestas dadas.

CAPITULO I

EL PROBLEMA DE INVESTIGACIÓN

En este primer capítulo se tiene como objetivo realizar el planteamiento del problema, formulación del problema, los objetivos generales y específicos, las limitaciones y el alcance del trabajo de investigación.

Planteamiento del problema

El desarrollo sostenido que han tenido las telecomunicaciones y las aplicaciones han modificado la visión que se tiene actualmente de la información y de la manera en que se puede estar enterado cada vez más al instante de sucesos que acontecen bien en nuestro vecindario o al otro lado del mundo. Y es que de la época en que comenzaba el desarrollo del internet, y su consecuente masificación, hasta la actualidad han ocurrido muchos eventos que de manera significativa han tenido un impacto en nuestra cotidianidad.

Los sistemas de información, cada vez más orientados a satisfacer las necesidades de cada usuario, han crecido de tal forma que ya el mundo actual no es concebible sin las ventajas que ofrecen las redes de telecomunicaciones y los aplicativos que usamos en nuestro día a día, de los cuales somos cada vez más dependientes.

Precisamente, a raíz de esa dependencia, es que se ha hecho cada vez más imperativo, tener a resguardo la información que obtenemos o enviamos a los más diversos lugares del planeta, la seguridad de dicha información es cada vez más imprescindible.

A la par que la tecnología va avanzando rápidamente cada año, las nuevas amenazas a la seguridad implican que las llamada red de redes va a permanecer en constante cambio tanto en su arquitectura como en su funcionamiento, esto motivado a que deberán implementarse nuevos mecanismos que procuren mantener la seguridad de los datos que manejamos en la web.

En la actualidad muchas empresas del sector público o privado fundamentan su funcionamiento o parte importante del mismo alrededor de redes internas y externas que le permiten prestar servicios cada vez más tecnificados y mejorar su respuesta para con sus potenciales usuarios, la facilidad de tramitar documentos a través de la internet es algo que no solo resulta cada vez más cotidiano, sino que no se concibe que en épocas relativamente recientes estos procesos eran exclusivamente manuales.

A medida que el crecimiento de Internet comenzó a explotar a comienzos de la década de 1990, los servicios ofrecidos en ese entonces por los proveedores eran

bastante limitados, generalmente ofrecían conectividad física, enrutamiento y servicios de registro, al mismo tiempo que servicios de sistema de nombres de dominio. El proveedor era el principal responsable de la seguridad del sistema de cara a lo externo y del circuito físico proporcionado a la organización, al igual que de su infraestructura y red principal.

Actualmente, los proveedores ofrecen un amplio espectro de servicios como parte de la oferta estándar de productos relacionados con Internet. Si una organización depende de su proveedor de servicios, para la administración de su plataforma de redes, dicho proveedor será el responsable de la seguridad de la información, sin embargo, si dicha organización, decide tomar en sus manos la administración de estos servicios, esta responsabilidad recaerá directamente sobre la organización.

En cualquier caso, es importante que en uno u otro sentido se tome conciencia de las funcionalidades y riesgos que implican estos servicios, así como de las formas que pueden sacar provecho de ello potenciales atacantes. En este punto es donde se deben tomar las decisiones adecuadas para bien elegir adecuadamente el proveedor de los servicios de Internet (ISP) o de los métodos que se escojan para proteger nuestra información.

En Venezuela, el tema de la seguridad de la información, ha cobrado especial auge en la últimas dos décadas, si bien, aun al día de hoy no es común que las organizaciones y/o instituciones tengan en su seno equipos especialmente contratados para mantener la seguridad informática, esto es norma por lo general en empresas de gran tamaño, bien sea del sector público o privado.

Para los entes y organismos de la Administración Pública Nacional de Venezuela funciona la Superintendencia de Servicios de Certificación Electrónica, que, tal como se expresa en su página web:

"Es un servicio creado mediante decreto Ley N° 1.204 de fecha 10 de febrero de 2001, sobre mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolívariana de Venezuela N° 37.148 del 28 de febrero de 2001".

Adicionalmente a sus servicios de implementación de modelo jerárquico de la infraestructura Nacional de Certificación Electrónica, también acredita, supervisa y controla a los Proveedores de Servicios de Certificación (PSC) y es el ente responsable de la Autoridad de Certificación Raíz en el estado Venezolano. Asimismo tiene como alcance proveer estándares y herramientas para implementar una tecnología de información óptima en la empresas del sector público, a fin de obtener un mejor funcionamiento y proporcionar niveles de seguridad confiables".

Para tratar temas relacionados a la Seguridad Informática, en primer lugar es importante conocer mas a fondo el tema, cuando mencionamos ese concepto. Claro que a este respecto, existen múltiples definiciones, y dicha discusión no forma parte de este documento.

Acerca de este concepto Pacheco expresa: (2009, p. 16)

"Tal vez una de las formas mas precisas de expresar la idea de seguridad de la información sea la siguiente: un conjunto de medidas de prevención, detección y corrección orientadas a proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos".

Se destaca la gran amplitud del espectro de conocimientos qué se busca abarcar con el mencionado concepto.

Dada la vigencia que han alcanzado los temas asociados a la seguridad de la información y que con el transcurrir del tiempo comenzó a extenderse a otras áreas, tal es así, que ha trascendido las fronteras de la informática propiamente dicha, elevando de alguna manera su alcance y propiciando la actualización constante de dicho concepto.

Con respecto a esto Pacheco define: (2009, p. 16) “Este hecho se basa en que la información va mucho más allá de la netamente procesada por equipos informáticos y sistemas, es decir, también abarca aquello que se piensa, aquello que está escrito en un papel, aquello que se dice, etcétera”.

Y luego complementa la información con la siguiente aseveración: “De esta manera, podemos determinar que este concepto incluye al anterior como caso particular, por el hecho de agregar otras áreas de dominio. Algunos temas no relacionados directamente con la informática, pero si con la información son, por ejemplo, los que tiene que ver con planes de contingencia y continuidad de negocios, valuación de activos, leyes y normas, políticas y procedimientos, etcétera”.

En el desarrollo del presente documento el enfoque específico se dará sobre los temas técnicos que sí están relacionados con la informática propiamente dicha, por lo que no se incluirán más que comentarios o anexos sobre otros tópicos.

En Venezuela la Administración Pública Nacional (APN), que dentro del marco de la estructura del estado, admite la centralización, entendiéndose esta como la acción de reunir o concentrar en un solo órgano, todos los asuntos de índole político y administrativo, es decir que existe un único órgano superior capaz de tener bajo su

mando todas las funciones, competencias y controles, con respecto a los demás órganos que integran la Administración Pública Venezolana.

Ahora bien, dentro del marco de la estructura de una Administración Pública centralizada, se encuentran diferentes niveles de organización que nos ayudan a entender la estructura de la APN, los cuales son:

1.La Administración Pública Nacional

2.La Administración Pública Estatal

3.La Administración Pública Municipal

La APN conforma el primer y más alto nivel dentro de la administración pública, se rige por las disposiciones de la Ley Orgánica de la Administración Pública (LOAP), con la finalidad de ampliar y organizar el estado atendiendo a la organización y la competencia de los poderes públicos establecidos previamente por la Constitución.

Enmarcado en la APN, como un ente que depende del Ministerio del Poder Popular para el Proceso Social del Trabajo, está el Instituto Venezolano de los Seguros Sociales (IVSS) que es una institución pública, cuya razón de ser es brindar protección de la Seguridad Social de todos los beneficiarios en las contingencias de maternidad, vejez, sobre vivencia, enfermedad, accidentes, incapacidad, invalidez,

nupcias, muerte, retiro y cesantía o paro forzoso y con calidad de excelencia en el servicio prestado, dentro del marco que lo regula.

En la actualidad el IVSS se encuentra en un proceso de adecuación de su Plataforma de Tecnología a fin de atender las necesidades de la población trabajadora y patronos que hacen uso de los servicios prestados por dicha Institución. En la procura de este objetivo, se propone el presente trabajo de investigación, que busca alcanzar las prácticas más adecuadas en materia de Seguridad de la Información y de esta manera ofrecer un servicio de calidad a los usuarios de los servicios que se prestan en Instituciones pertenecientes a la Administración Pública.

Dado que los usuarios del Instituto Venezolano de los Seguros Sociales, corresponden a sectores particularmente vulnerables de la población (adultos mayores) y adicionalmente maneja información asociada a las empresas registradas que deben cumplir con los pagos al instituto, corresponde entonces la implementación de todos los mecanismos posibles para garantizar que los datos que corresponden a la población, tengan los mencionados usuarios garantía de confidencialidad, integridad y disponibilidad.

Es importante acotar que aun cuando no se puede garantizar el 100% de la seguridad a un sistema, sin embargo, es importante tomar todas las medidas que estén al alcance para ofrecer garantía de que en caso de alguna eventualidad, los efectos negativos de dicho suceso, bien sea un ataque a la red, perdida de información, intencional o no, filtración de datos a manos indebidas, etc., pueden ser mitigados por las medidas tomadas en pro de la seguridad de la información de una determinada organización.

Por todo lo antes mencionado, se considera importante la implementación de estándares y mejores prácticas, para de esta manera procurar mantener la operatividad en niveles cercanos al 100% del tiempo. En este sentido se propone un modelo de madurez, que a Guía de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) nos define de la siguiente manera 4.1 (cp *Software Engineering Institute* (SEI), 2007), “Plan evolutivo para pasar de un proceso *ad-hoc* o caótico a uno maduro” (p. 4) que permita medir el desarrollo de los procesos administrativos que sirven de fundamento para dicho planes.

Los modelos de madurez responden a la necesidad no solo de valorar el estado actual de la Institución, sino que permite desarrollar una estrategia para identificar, implementar y optimizar capacidades críticas.

Formulación de las interrogantes de la investigación

La interrogante principal de la investigación se puede resumir en el siguiente enunciado:

¿Cual es el Nivel de Madurez asociado a la seguridad de la información que permitirá a las organizaciones y/o instituciones del sector público en Venezuela garantizar niveles adecuados de Seguridad en el manejo de la información?

A partir de la anterior interrogante, se derivan las siguientes preguntas:

1)¿Que problemática se origina del desconocimiento de las fallas en materia de Seguridad Informática en las Instituciones del sector público?

2)¿Que acciones se deben tomar para controlar el tráfico que se genera en una red corporativa y tener una adecuada gestión de las situaciones que se presenten, que garantice tomar las medidas tendientes a actuar de manera proactiva?

3)¿Que se necesita para manejar la gestión de la seguridad informática de acuerdo con los estándares y mejores prácticas establecidas?

4)¿Que se debe establecer como mecanismo para medir el nivel de madurez de la institución en estudio?

5)¿Que mecanismos de verificación se pueden realizar para garantizar que el Modelo de Madurez a implementar sea el adecuado a la Plataforma en estudio?

Objetivos de la Investigación

Objetivo General.

Proponer un Modelo de Madurez de Seguridad de la Información para el Monitoreo y Análisis del Tráfico de redes en la Administración Pública Nacional de Venezuela.

Objetivos Específicos.

1. Identificar las posibles falencias en materia de Seguridad Informática, en instituciones pertenecientes a la Administración Pública Nacional.

2. Establecer los mecanismos que permitan tener un control pormenorizado del tráfico que se genera en una red determinada y establecer las métricas que permitan determinar cuándo se presenten situaciones anómalas y actuar en previsión de fallas.

3. Determinar el estado actual de la Seguridad Informática en instituciones públicas y diagnosticar estado actual en relación con los estándares y mejores prácticas establecidas.

4. Diseñar las etapas del modelo de madurez propuesto teniendo como premisa los estándares y mejores prácticas existentes.

5. Validar el modelo de madurez obtenido mediante su aplicación en el IVSS, esto contando con el juicio experto de personal adscrito a dicha institución.

Justificación e Importancia de la Investigación

Tal como se ha venido expresando en el presente documento, la importancia de Seguridad de la Información en la actualidad es vital, se precisa conocer con exactitud cuál es el estado real en esta materia que tiene una Institución y que pueda dar una máxima garantía de confiabilidad a sus usuarios y a la nación en general.

En este sentido, se precisa conocer el estado actual de la Seguridad de la Información y que medidas deben tomarse para que la institución pueda obtener incluso certificaciones para organizaciones, que pudiéramos considerar el estado ideal.

Esta investigación tiene por finalidad proponer un modelo de madurez para la evaluación del tráfico de red de una Institución Pública, específicamente el IVSS y establecer los mecanismos necesarios para, que de una manera automatizada se puedan obtener lecturas de situaciones que pudieran considerarse anómalas y que

se constituirían en potenciales vulnerabilidades y/o amenazas que comprometerían la prestación del servicio de una Institución.

Una vez establecido que es necesario contar con herramientas que permitan tener un control automatizado del monitoreo y análisis del tráfico de red y que se pueda evaluar el estado actual con la implementación de un modelo de madurez, podemos fundamentar en las siguientes premisas la justificación e importancia de la investigación:

- Comparar: Una vez que se realice el trabajo de identificar el estado actual en materia de monitoreo y análisis de tráfico se puede determinar dónde deben aplicarse los correctivos pertinentes.
- Desarrollo estratégico: Se determina cuál es la estrategia a seguir para establecer como parámetro el Modelo de Madurez recomendado y el porqué de la pertinencia de este modelo y no otro.
- Aseguramiento de la calidad: La actualización permanente de el mencionado modelo, procura mantener en su estado óptimo las mejoras implementadas.

Dentro de las diversas áreas temáticas de sistemas de información, la presente investigación se sitúa dentro de las tecnologías de información (hardware y software)

y herramientas de detección y prevención de Intrusos, enfocados a seguridad de la información.

Alcance y Limitaciones

El ámbito del presente trabajo de investigación lo conforma la Plataforma Tecnológica del Instituto Venezolano de los Seguros Sociales, específicamente el área correspondiente a la Dirección General de Informática (DGI) Inmersa en esta Dirección se trabaja directamente con la Unidad de Seguridad Informática (USI) Se cuenta con acceso a información pertinente para el trabajo a desarrollar, sin embargo es de hacer notar que por ser parte de lo que se debe considerar como información confidencial, esto ya de por si es una limitación.

Igualmente, se tuvieron las impresiones de personal de diversas instituciones del estado que están inmersas dentro del Marco de Interoperabilidad, en materia de seguridad de la información.

Entre las limitaciones encontradas tenemos:

- La documentación actual en cuanto al tema es escasa.
- La confidencialidad de la información pudiera considerar como una de las principales trabas en el desarrollo del presente trabajo.

- Costos asociados a las horas/hombre que serán necesario emplear en la reunión de expertos de diversas áreas, para tratar los temas relacionados.
- El costo de los materiales de impresión y disponibilidad de insumos de ese mismo rubro.

Resultados obtenidos de la investigación:

- Descripción de las debilidades actuales en materia de análisis y monitoreo de tráfico y establecer las contra medidas a tomar para orientar y encauzar dichas debilidades, para el fortalecimiento de las mismas.

- Control del tráfico que se genera en la red a través de Marco de Trabajo que haga lecturas al momento del comportamiento de dicho tráfico.

- Diagnóstico de las necesidades actuales de prevención y detección de intrusos a través del monitoreo pro activo de las redes y el uso de herramientas especializadas.

- Descripción de las falencias que se derivan de la problemática existente en el monitoreo de redes en relación con los estándares y mejores prácticas establecidas.

- Descripción de las etapas del modelo de madurez a implementar, que cumpla con los estándares y mejores prácticas existentes en Seguridad de la Información.

Fases a establecer para determinar las métricas que indiquen el estado de la red en condiciones de operatividad y establecer los umbrales que alerten de anomalías en el comportamiento usual.

- Establecer un Modelo de madurez con base a los estándares y mejores prácticas existentes que permita minimizar los riesgos asociados a potenciales ataques a redes institucionales. Haciendo uso de soluciones automatizadas, manteniendo y probando de forma continua el estado de actualización de dichas herramientas.

- Modelo de madurez validado que satisface las necesidades del IVSS y que le permita contar con herramientas adicionales a las existentes y que van a contribuir a mitigar las potenciales vulnerabilidades y tomar los correctivos en caso de ser necesario.

CAPÍTULO II

MARCO TEÓRICO

En el presente capítulo se hace referencia a los aspectos teóricos que respaldaran la investigación propuesta. La mencionada investigación sitúa los conceptos, bases teóricas, referencias teóricas, conceptos metodológicos y herramientas utilizadas para la propuesta del modelo.

Antecedentes de la Investigación

En el desarrollo del presente trabajo de grado se tomaron como referencia para los antecedentes de la investigación los siguientes documentos:

Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en la Universidades en la Universidad Simón Bolívar por Marianella Villegas (2008), cuyo objetivo fue: “Diseñar una propuesta de un Modelo de Madurez Organizacional con respecto a la Administración de la Seguridad de la Información (MMAGSI), para Universidades Venezolanas ubicadas en la Región Capital. La metodología la metodología aplicada para el logro de este objetivo es una investigación de campo, de carácter exploratorio; además se aplicó el método Delphi para validar el modelo de madurez construido a través de las entrevistas realizadas a personal experto y consultores en Seguridad de la Información.
Por otra parte, se diseñó un instrumento de medición con la finalidad de determinar en qué nivel de madurez está ubicada una universidad en el modelo MMAGSI”.

El principal aporte de esta investigación, debido a su diseño documental, fue la bibliografía consultada para su elaboración, las normas y estándares utilizados, así como todos los procesos relativos modelo de madurez.

Palabras clave: Gestión, Seguridad de la Información, Nivel, Madurez.

Desarrollo de un Modelo de Madurez para las Contingencias y Recuperación de la Información en las Pequeñas y Medianas Empresas del Sector Salud en Venezuela en la Universidad Católica Andrés Bello de Felipe Hernández (2011), cuyo objetivo fue "La propuesta de un Modelo de Madurez para las pequeñas y medianas empresas (PYMEs) venezolanas del sector salud, con el fin de proteger la información y la tecnología, que en algunos casos son los activos más valiosos de la información frente a posibles amenazas que ofrece permanentemente el medio ambiente tecnológico.

Es de importancia vital reducir al mínimo los efectos adversos causados por los desastres y ayudar a prevenir la aparición de otros en el futuro".

El principal aporte de esta investigación lo constituye la Metodología empleada y las analogías que se pudieron realizar en la implementación del Modelo de Madurez.

Palabras clave: Sistemas de Información, Modelo Conceptual, Modelo de Madurez y seguridad de la Información, PyMes

Modelo de Gestión de Procesos de Servicios de Tecnología de Información Basado en Librerías de Infraestructura de Tecnologías de Información (ITIL) para la Administración Pública Nacional en la Universidad Católica Andrés Bello de Lynmar Ortiz(2012) que plantea el siguiente objetivo: "..El Desarrollo de un modelo de gestión de procesos de servicios tecnológicos basado en Librerías de Infraestructura de Tecnologías de Información para la Administración Pública Nacional. Se utilizó como marco metodológico el método Investigación - Acción de

Baskerville (1999), el cual consta de cinco (5) fases: Diagnosticar, Planificar la acción, Tomar la acción, Evaluar y Especificar el aprendizaje".

El principal aporte de esta investigación fue la consulta del marco legal, por tratarse de investigación desarrollada en el ámbito de la Administración Pública Nacional.

Palabras clave: Librerías de Infraestructura de Tecnologías de Información, Tecnologías de Información, Administración Pública Nacional, Modelo, Centro Nacional de Tecnologías de Información, Investigación-Acción, Procesos

Modelo de Madurez y Capacidad de Implementación de Gobierno Electrónico en Instituciones Públicas en la Universidad Técnica Federico Santa María de Gonzalo Valdéz (2010) que plantea como premisa lo siguiente: "Surge la necesidad de medir el grado de preparación que poseen las instituciones públicas para incorporarse a iniciativas de integración de información de distintos servicios públicos. Se plantea la hipótesis de que un modelo de madurez de gobierno electrónico, que integre la evaluación de capacidades tecnológicas, organizacionales, operacionales y de capital humano, permitirá al gobierno realizar evaluaciones efectivas, estandarizadas y replicables".

De este investigación se tuvieron aportes en materia de bibliografía principalmente, en torno al tema de Modelos de Madurez, igualmente se analizó la manera de tratar el tema en torno al Gobierno Electrónico y los aportes que este paradigma puede dar para una eficaz gestión de recursos.

Palabras Clave: Gobierno Electrónico, Modelos de Madurez y Capacidad.

Aplicación de un Modelo de Madurez de Gerencia de Proyectos para una Institución Bancaria en la Universidad Católica Andrés Bello de María Barrios (2004), esta es una tesis de grado que procura los siguientes objetivos: "Investigación de tipo evaluativa la cual consistió en aplicar el modelo de madurez del Dr. Harold Kerzner (PMMM) para evaluar y diagnosticar el nivel de madurez en

Gerencia de Proyectos de la Institución Bancaria en estudio a través de la adaptación de los instrumentos de medición propuestos por el.

El estudio resulta de gran relevancia ya que permite determinar las capacidades y habilidades de la organización en Gerencia de Proyectos para identificar fortalezas y proponer recomendaciones para el mejoramiento continuo a favor de lograr ser más competitivos en un mundo financiero agresivo y cambiante".

El principal aporte de esta investigación fue el estudio de la aplicación de los Modelos de Madurez en el ámbito de la gerencia y por ende fue de gran valor para aplicar dicho enfoque en el tema de gestión de la seguridad.

Palabras clave: Gerencia de Proyectos, Banca, Modelo de Madurez, Gerencia.

Actualmente, existen metodologías, estándares, modelos de madurez y guías que pueden ayudar a una organización a mejorar su modo de operar. Los modelos de madures constituyen una evolución de las metodologías para gestionar la calidad de la organización. Fueron concebidos inicialmente para la industria del software, pero actualmente su área de aplicación es muy diversa.

La implementación de los modelos de madures en organizaciones de diversos tamaños permite obtener resultados medibles y establecer planes y/o estrategias a seguir para la mejora constante en diversos procesos de una organización determinada, para esto es preciso contar con personal calificado, que permitan la emisión de un juicio experto en el área de estudio. Se procura entonces realizar las recomendaciones pertinentes que puedan servir de referencia para su aplicación en el IVSS a partir del estudio de reconocidos modelos de madurez y de implementaciones previas.

El mapa mental del marco teórico de la presente investigación se encuentra representado en la Figura 1.

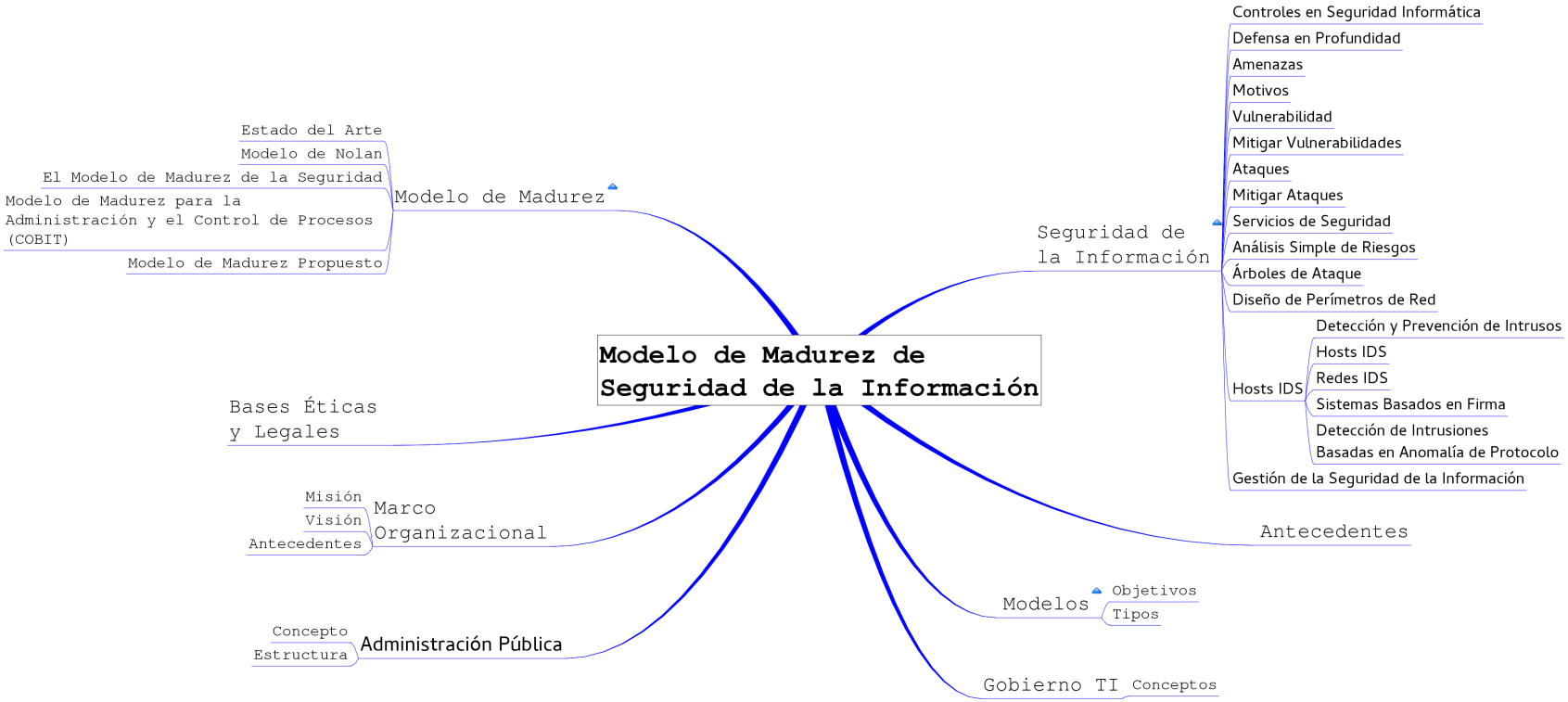

Figura 1: Mapa mental del marco teórico. Fuente Elaboración propia.(2016)

Bases Teóricas

La elaboración del marco teórico tiene como finalidad estructurar los elementos e instrumentos teóricos que permiten orientar la investigación, la cual se emprende en busca de explicaciones e interpretaciones relacionadas con la seguridad de la información y más específicamente en el área del monitoreo pro activo del tráfico de redes , lo que permite conocer con mas detalle conceptos fundamentales para la comprensión del presente trabajo de investigación.

La seguridad

En primer lugar, es preciso establecer un concepto de seguridad, que es tema central del presente trabajo, según definición de la Real Academia Española, tomada de su página web (RAE) (2016) “El concepto de seguridad va asociado a la no presencia de riesgo, y también está determinado por el grado confianza que se tiene en algo o alguien. Sin embargo, el mencionado termino puede tomar diversos significados dependiendo del área o ámbito en que se esté haciendo referencia a la seguridad”.

En líneas generales se puede indicar que la seguridad la percibimos como un estado de bienestar.

Seguridad de la Información

Tal como se mencionó con anterioridad se han escrito diversos conceptos sobre seguridad de la información, Pacheco (2009, p. 18) indica lo siguiente: “definiremos como Seguridad de la Información, esa frase tan conocida que solemos repetir continuamente y que tanto misterio despierta: seguridad de la información. Con más o menos palabras, se la define como el conjunto de medidas preventivas, de detección y de corrección destinadas a proteger la integridad, confidencialidad y disponibilidad de los recursos informáticos”.

En términos generales es un concepto que es aceptado por la mayoría de los autores, donde se puede observar en la segunda parte de la definición que contiene los tres pilares de la seguridad de la información: integridad, confidencialidad y disponibilidad, también conocidos por sus siglas en inglés como la tríada CIA (*Confidentiality, Integrity, Availability*, en español Confidencialidad, Integridad y Disponibilidad), tal como se ve en la siguiente figura:

Figura 2: Tríada CIA (Confidencialidad, Integridad y Disponibilidad). Fuente: (Pacheco: 2009)

Ahondando un poco más en el concepto de Seguridad de la Información, se puede definir cada uno de los conceptos que están contenidos en el mismo, hablando de Confidencialidad, Pacheco (2009, p. 22) indica lo siguiente: “Se habla de confidencialidad cuando se hace referencia la característica que asegura que los usuarios (sean personas, procesos, etcétera) no tengan acceso a los datos a menos que estén autorizados para ello”. Por otra parte, Pacheco (2009, p. 22) dice con respecto a la integridad: “Toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos autorizados. Finalmente, expresa que : “La disponibilidad garantiza que los recursos del sistema y la información estén

disponibles sólo para usuarios autorizados en el momento en el que lo necesiten" (p. 22).

En el entorno de las organizaciones, independientemente del tamaño que sean, la seguridad de la información garantizan que la gestión empresarial es inteligente, para prevenir las amenazas de la era digital. En este mismo orden de ideas, la seguridad es un medio para consolidar la consecución de un fin, que no es otro que el de la confianza que pueda transmitir la organización a sus clientes o usuarios, de que la información que está siendo gestionada por dicho ente está a buen resguardo.

Según la norma de la Organización Internacional de Normalización conocido como ISO por sus siglas en inglés, 27002 (2005) "La seguridad de la información es la protección de la información contra una gran cantidad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de las inversiones y oportunidades de negocio".

Cheswick, W. Y Bellovin, S. (1994, p. 45) comentan: "Hablando ampliamente, la seguridad es evitar que alguien haga cosas que no quieres, que haga o no desde tu ordenador o alguno de sus periféricos " para estos expertos en el área de seguridad, la seguridad radica en mantener el control.

Igualmente, Schneier (2002, p. 28) expresa: “La seguridad es un proceso, no un producto”, es decir la seguridad no implica un conjunto de medidas a tomar.

Aceituno (2004, p. 56) define la seguridad de la información como “Las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los Sistemas de Información, incluyendo hardware, software, firmware, y aquella información que procesan, almacenan y comunican”.

Finalmente, en este orden de ideas, Gómez, A. (2006, p. 63) define la seguridad de la información como “La medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios al sistema”.

Controles en Seguridad Informática

Tal como se ha descrito con anterioridad, el objetivo fundamental de la seguridad informática es fortalecer una o varias de las características de seguridad mencionadas, para de esta manera mitigar los efectos producidos por las amenazas y vulnerabilidades. El riesgo de sufrir un incidente de seguridad nunca lo vamos a

poder eliminar por completo, pero si se va a reducir de manera considerable para que de esta manera se pueda hacer tolerable por nuestra organización.

Los controles en el área de la Seguridad de la Información, según Laudon, K. Y Laudon, J. (2002, p. 38) “consisten en todos los métodos, políticas y procedimientos para asegurar la protección de los archivos de la institución, la precisión y la confiabilidad de sus registros y la adherencia operativa a las normas de la administración”.

En este mismo orden de ideas, los autores Álvarez, G., y Pérez, P., (2004, p. 55) dicen que; “están orientados al diseño y utilización del software, la seguridad de los archivos y la base de datos de la institución. Además, de una combinación de software y procedimientos manuales; por tanto son globales y se aplican en todas las áreas. Los controles generales incluyen los de proceso de implantación del sistema, para software, los físicos para el hardware, los de operaciones de computo, los de seguridad de datos y las disciplinas, normas y procedimientos administrativos”:

Con respecto al tema, Pacheco (2009, p. 19) indica lo siguiente: “Estos controles pueden clasificarse según dos criterios: Por un lado dependiendo del momento en el que se actúa, se tendrán controles preventivos, disuasivos, detectivos, correctivos y recuperativos. Los preventivos y disuasivos toman acción en momentos anteriores al

incidente, con el objetivo de evitarlo. Los detectivos buscan detectar el incidente en el momento en que éste está ocurriendo. Finalmente, los correctivos y recuperativos tienen lugar una vez que el incidente ocurrió".

Esto se puede visualizar en la siguiente figura:

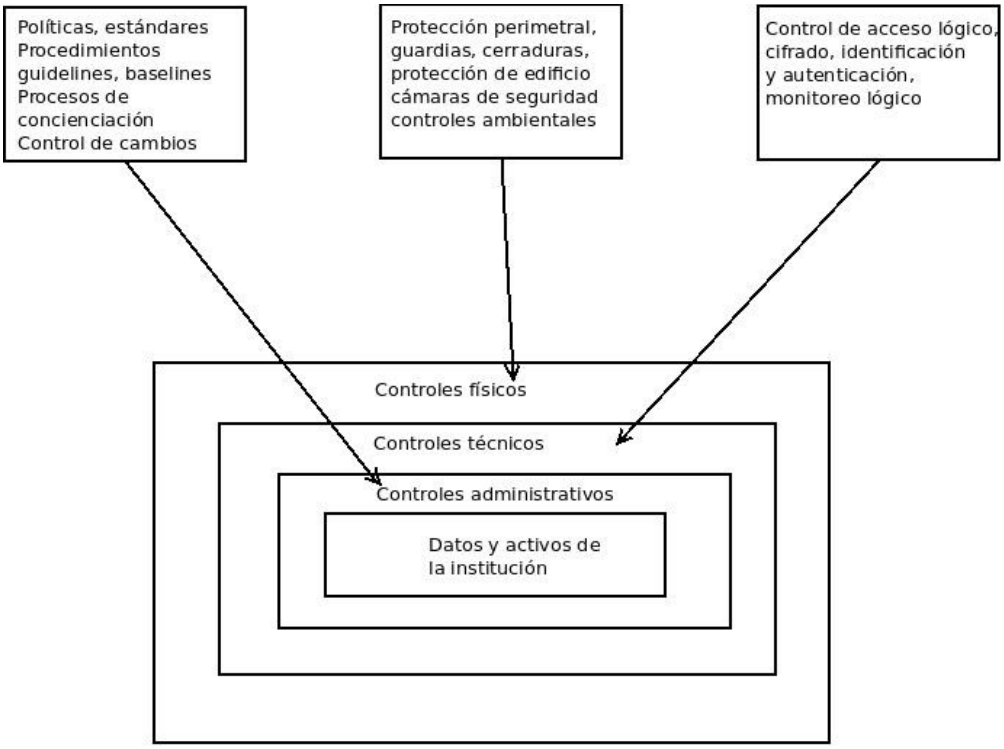

Figura 3: Controles divididos según el momento del incidente Fuente (Pacheco: 2009)

En otro orden de ideas, según el tipo de recursos utilizados para ejercer los controles, se van a clasificar en físicos, técnicos o lógicos y administrativos. Con respecto a este tipo de controles Pacheco (2009, p. 20) indica lo siguiente: “Los controles físicos serán aquellos que implementen medidas de seguridad física, como por ejemplo, cerraduras electrónicas, sistemas de acceso biométrico, etcétera. Los controles técnicos o lógicos implementan usualmente, medidas de carácter tecnológico, como sistemas de , detección de intrusos, seguridad de las aplicaciones y sistema operativo, etcétera. Finalmente, son muy importantes aunque muchas veces desvalorizados, los controles administrativos. La importancia de estas medidas radica en que son las que suelen determinar, en función de políticas de seguridad, las configuraciones que deben cumplir el resto de los controles, por ejemplo, las configuraciones de los controles de acceso y las reglas (desde el punto de vista de las políticas de acceso que deben implementarse en un firewall”.

Como puede inferirse, esos controles pueden pertenecer a más de una categoría a la vez muchas veces, según el punto de vista que se tenga en cuenta. Para analizar la efectividad de esos controles se realizan distintos análisis de seguridad, conocidos usualmente como, evaluación de vulnerabilidades (*Vulnerability Assessment*) y Hacking ético (*Ethical hacking*).

Defensa en profundidad

En el área militar se utiliza el término defensa en profundidad para denotar el uso de varias líneas de defensa consecutivas, esto en contraposición de una sola barrera defensiva muy fuerte. La idea de este tipo de implementación se basa en que un potencial atacante perderá fuerzas al superar cada barrera y además eventualmente dispersará sus recursos y potencia, debilitándose. Así, quien se defiende puede centrar sus esfuerzos en la reorganización y acción estratégica. En el área de la seguridad de la información, se establecen de manera análoga las barreras defensivas en los distintos sistemas informáticos y se establecen perímetros de seguridad con la finalidad de proteger de manera más eficiente nuestras plataforma tecnológica.

Un extracto del documento creado por la Dirección Central de la Seguridad de los Sistemas de Información del Gobierno Francés (SGDN/DCSSI), cuyo sitio web es www.ssi.gov.fr dice así:

“La defensa en profundidad del sistema de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren toda la profundidad del sistema”.

Esto implica, que todos los elementos de seguridad, deben estar correlacionados e interactuar entre si de manera coordinada.

También se toma de la misma web, lo siguiente: “El término profundidad debe entenderse en su sentido más amplio, es decir, en la organización del Sistema de Información, en su implementación y, por último, en las tecnologías utilizadas.

Se tiene que implementar la seguridad en diversos anillos que van desde el borde o perímetro, hasta los niveles mas álgidos, lo que se conoce como el núcleo de los datos de la institución.

“Se trata, por lo tanto, de permitir acciones de neutralización de los atentados contra la seguridad, al menor costo, mediante la gestión de los riesgos, un sistema de informes, la planificación de las reacciones y el enriquecimiento permanente gracias a la experiencia adquirida”.

Para hacer una aplicación a una plataforma tecnológica, se deben tomar como referencia modelos ya existentes que se adapten de la mejor manera a la relación costo-factibilidad.

La empresa Microsoft, ha difundido a través de sus canales de entrenamiento el siguiente esquema, que puede resultar muy didáctico:

- Políticas, procedimiento y concienciación.
- Seguridad física.
- Seguridad del perímetro.
- Seguridad de la red.
- Seguridad del equipo.
- Seguridad de la aplicaciones.
- Seguridad de los datos.

Se puede concluir sobre este punto, que el uso de las técnicas de defensa en profundidad constituye una gran ayuda y puede ayudar a implementar la seguridad de una manera efectiva, basándonos en este punto se puede tomar como referencia al momento de realizar la evaluación del estado actual de la seguridad en el IVSS y de los resultados obtenidos elaborar el plan a seguir para orientar las medidas de seguridad al uso de los mejores prácticas dictaminadas por los expertos.

Amenazas

Una amenaza conforma una brecha que puede ocasionar un perjuicio a la seguridad de la información, las amenazas se constituyen como tales a partir de vulnerabilidades, esto significa que exista una amenaza debe haber una vulnerabilidad y que por lo tanto se puede explotar.

Diversas situaciones, tales como el incremento de la ingeniería social, la falta de conocimiento y concienciación de los usuarios en el uso de los elementos de la tecnología, y sobre todo la posibilidad de obtener lucro de ataques, han provocado que en los últimas décadas, los ataques intencionales sean muy frecuentes y llegan a constituir una verdadera pesadilla para los administradores de seguridad de organizaciones e instituciones.

Según Stallings, W., (2004, p. 42), son “una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que podría explotar una vulnerabilidad”.

Es importante destacar que las amenazas a un sistema de información, no son exclusivamente posibles desde un ente externo a nuestra Institución, sino por el contrario, estadísticamente se ha demostrado que un porcentaje elevado de dichos

ataques provienen de fuentes internas, bien sea un empleado molesto, usuarios con conocimientos de informática, o la ya mencionada impericia de los usuarios para dar el correcto uso a los elementos de la tecnología que se tiene actualmente presente en todos los ámbitos de nuestra vida, tanto laboral como personal.

Ahora bien, ¿quién podría atacar una plataforma tecnológica? Al respecto Bauer, M. (2005, p. 38) emite la siguiente reflexión: “Cuando se considere a los potenciales atacantes, es importante tomar en cuenta dos cosas. Primero, al menos cada tipo de atacante presente algún nivel de amenaza a cada computador conectado al Internet. Los conceptos de distancia, lejanía y oscuridad son radicalmente distintos en Internet que en el mundo físico, en términos de cómo se apliquen a la fuga de avisos de atacantes aleatorios. Teniendo una presencia en Internet “desinteresada” o de “bajo tráfico” no hay protección contra todos los ataques de extraños”.

De este modo, es poco probable que grupos antigubernamentales, o de índole política, ataquen de manera premeditada la plataforma de una empresa pequeña o mediana, con la finalidad de provocar algún daño. Sin embargo, que este ataque suceda, no es del todo descartable tomando en consideración, que la intrusión pueda tener como objetivo realizar el ataque desde un equipo presente en la empresa de mediano tamaño, para de este modo intentar eliminar el rastro de su acción.

Luego, Michael Bauer (2009, p. 40) indica lo siguiente: “Lo segundo a considerar en la evaluación de amenazas es que es imposible anticiparse a todas las probabilidades o incluso a todos los tipos de atacantes. No es posible anticiparse a todos los caminos de ataque (vulnerabilidades). Esto es correcto; el análisis de amenazas no es predecir el futuro, es pensar sobre ello y analizar las amenazas con más profundidad que “solo alguien quiera entrar a un sistema por alguna razón”.

En vista de esto, una vez más se reitera que no es posible anticiparse a todo, lo que si debe hacerse es tomar algunas medidas que resultan razonables para maximizar la conciencia de los riesgos que resultan evidentes. Los riesgos que no estén a la vista, pero deben ser tomados en cuenta y aquellos riesgos que no serían un problema pero pueden contrarrestase de manera sencilla.

Adicionalmente, en el proceso de analizar esos riesgos, también es posible identificar aquellas amenazas que son inviables de proteger aun cuando sepamos que son importantes. La importancia de esto radica en crear planes de recuperación contra estas situaciones.

Motivos

Muchas amenazas son bastante evidentes y fáciles de comprender. Es conocido que un potencial competidor en un mundo de negocios quiere realizar transacciones para

ganar más dinero y tener más presencia que sus rivales, es aquí donde un potencial ex empleado descontento, que quiera tomar venganza por haber sido despedido pudiera querer tomar acciones en contra de sus antiguos empleadores.

Otros motivos, no son tan fáciles de establecer, aunque raramente se dirige directamente en el análisis de las amenazas, con respecto a este punto Bauer (2009, p. 41) dice: "... hay algún valor discutible en los motivos que incitan a las personas a cometer delitos informáticos. Ataques sobre la confidencialidad de los datos e integridad, integridad de sistemas y disponibilidad de los sistemas corresponde respectivamente a sus equivalentes en la vida real de espionaje, fraude, romper y asaltar, sabotaje".

Tal como sucede en ámbitos distintos a la informática, los criminales de delitos informáticos son conducidos por los mismos motivos que los criminales de la vida real, si bien es cierto que en diferentes proporciones.

Vulnerabilidad

Un riesgo no es relativo acerca de activos y atacantes. Dicho de otra manera, si un activo no tiene vulnerabilidades (lo cual en la práctica no es factible), no hay riesgo y no importaría cuantos atacantes haya.

Para Bauer (2009, p. 43) : “La vulnerabilidad sólo representa un ataque potencial, y así, se mantendrá hasta que alguien sepa cómo explotar dicha vulnerabilidad en un ataque con éxito. Ésta es una importante distinción, pero se admite que en el análisis de amenazas es común conocer de las vulnerabilidades y ataques actuales de manera simultánea.

Con respecto al concepto de vulnerabilidad, Aceituno (2006, p.32) expresa: “La vulnerabilidad es la evaluación objetiva de la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado. Para conocer la probabilidad se hacen estadísticas basadas en sucesos pasados elaboradas a partir del número de casos favorables y el número de casos posibles”.

Según Gómez, L., Farías-Elinos, M., Mendoza, M., (2003, p. 72) señalan que vulnerabilidad: “Es la posibilidad de sufrir algún daño o perdida”, en tanto que Carracedo J., (2004, p. 45) opina que “Los riesgos de la información son: perdida, mal uso no intencional y deliberado, exposición o daño que sufre la información cuando es resguardada en dispositivos tecnológicos”.

En la casi totalidad de los casos, es potencialmente peligroso no tener en cuenta una vulnerabilidad conocida porque todavía no haya sido atacada, la cuestión radica

entonces en que no porque una vulnerabilidad no haya sido explotada, no deban tomarse las correspondientes medidas.

El peor escenario es que una vulnerabilidad digamos de código de software sea explotada en Internet, en un simple script o incluso un programa con interfaz, antes de que los programadores tengan el parche que corrija la mencionada vulnerabilidad.

Según Bauer (2009, p. 45), es preciso conocer, identificar y orientar lo siguiente con respecto al tema de las vulnerabilidades:

- Vulnerabilidades que claramente son aplicables en un sistema y deben ser atenuadas inmediatamente.

- Aquellas vulnerabilidades que probablemente se puedan aplicar en el futuro y contra las que se deben crear planes de choque.

- Todas las vulnerabilidades de las que se tiene muchas probabilidad de dar problemas más adelante, pero que son fáciles de mitigar.

En este mismo orden de ideas, Oppleman, V., Friedrichs, O., Watson, B., (2006, p. 286) establecen las siguientes clases de vulnerabilidades:

- Ataques contra la información sensible.

- Ataques contra la aplicación desde usuarios locales.

- Ataques contra la aplicación desde bibliotecas, terceros y el entorno de ejecución de la aplicación.

A su vez, estas vulnerabilidades se ramifican en las siguientes, que por lo general están dentro de alguna de las tres categorías anteriores, aun cuando no se trata de una lista completa sobre cada tipo de vulnerabilidad, si nos da una idea de cómo pueden subdividirse:

- Validación de entrada: casi todas las vulnerabilidades están causadas por este tipo de defecto programático. En pocas palabras, significa validar apropiadamente los datos proporcionados por el usuario o la aplicación.

- Inyección SQL y concatenación de cadenas: Una forma especializada de error de validación de entrada es aquel en el que los datos de entrada desde un lenguaje se emplean para generar datos de salida en otro. Una validación y generación correcta de estos lenguajes de salida resulta crítica.

- Desbordamiento o sobrecarga de buffer: También suele ser el resultado de errores en la validación de los datos de entrada, en el que la ejecución del programa se trastoca empleando un conocimiento especial sobre los métodos que emplean los

lenguajes internos con respecto a la reserva de memoria y al almacenaje en la plataforma objetivo específica.

- Condiciones de carrera: Ataques basados en suposiciones sobre el orden del flujo de ejecución de una aplicación o la sincronización de recursos interdependientes.

- Agotamiento de memoria y recursos: Errores de reserva de memoria o recursos que, si se aprovechan, pueden provocar la denegación de servicio.

- Vulnerabilidades futuras: Otros ataques avanzados contra aplicaciones, así como preocupaciones de entrada.

Mitigar las vulnerabilidades

Una estrategia que debe tomarse en cuenta para defender la información de activos es aquella que tienda a eliminar o mitigar las vulnerabilidades. Un buen ejemplo de esto son los conocidos parches de software.

Considerando este tema, un mejor ejemplo de mitigar vulnerabilidades de software es la codificación defensiva; ejecutando el software a través de una serie de filtros, que por ejemplo, verifiquen los limites, asegurando así que el software no es vulnerable a los ataques de desbordamiento de bufer.

Bauer (2009, p. 53) expresa: "...mitigar vulnerabilidades es simplemente otra forma de asegurar la calidad. Arreglando cosas que se han diseñado pobremente o simplemente con fallos se mejora la seguridad".

Ataques

En el desarrollo del presente documento, se ha estado hablando de las potenciales amenazas que se ciernen sobre los sistemas informáticos y en general sobre la plataforma tecnológica de la una organización, ahora pasamos a describir en que consisten esas amenazas, de que debemos proteger los activos de la Institución, en que consisten dichas amenazas o ataques que suelen ser la razón de ser de equipos de seguridad informática en organizaciones de diversos tamaños.

Un ataque informático suele ser un método a través de cual una persona, o grupo de personas, haciendo uso de aplicaciones y/o sistemas informáticos, intentan generar perturbaciones en el correcto funcionamiento, controlar, o aun dañar por completo otro sistema, que bien puede ser una red, un aplicativo, una base de datos, etcétera.

Con respecto al concepto de ataque informático Stallings (2004, p.48) establece:, "un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema".

Como es de suponer, no todos los ataques son de la misma naturaleza. Tomando el punto de visto técnico para hacer una clasificación de los ataques Pacheco (2009, p. 238) establece la siguiente clasificación:

- Ataques al sistema operativo: Los ataques al sistema operativo constituyen un clásico de la seguridad. Desde esta perspectiva, la búsqueda de fallas se realizará en lo concerniente al propio sistema base de todo el resto del software, de tal forma que muchas veces, independientemente de lo que se encuentre por encima, se podrá explotar y tomar control del sistema en el caso que sea vulnerable.

- Ataques a las aplicaciones: Aquí la variedad es mayor, existen múltiples piezas de software y programas de todo tipo y tamaño disponibles en el mundo. Por supuesto, entre tantos millones de lineas de código, se producen necesariamente errores. Para los ataques a las aplicaciones también se tendrá en cuenta la masividad de uso. Esto implica que un programa manejado por millones de personas para leer archivos del tipo Formato de Documento Portatil (PDF) será un objetivo mas usual que uno que usan unos pocos para editar cierto tipo de archivos específicos de un formato menos conocido y utilizado.

- Errores en configuraciones: El caso de las configuraciones, ya sean del sistema operativo o de las aplicaciones también constituye un punto sensible, dado

que por más seguro que sea un software, una mala configuración puede tornarlo tan maleable como un papel.

- Errores en protocolos: Otro gran problema al que podemos enfrentarnos es que se encuentren errores en protocolos. Esto implica que, sin importar la implementación, el sistema operativo, ni la configuración, algo que se componga de dicho protocolo podrá ser afectado. El ejemplo más clásico de todos es tal vez el del *Transmision Control Protocol / Internet Protocol (TCP/IP*), una suite de protocolos tan efectiva y flexible que, luego de más de tres décadas de existencia, aún perdura y continua siendo utilizada.

McNab (2008, p. 37) hace la siguiente clasificación: “En un alto nivel, los atacantes basados en Internet pueden dividirse en los dos grupos siguientes”:

- Atacantes oportunistas que rastrean grandes espacios de direcciones en busca de sistemas vulnerables.

- Atacantes decididos que atacan sistemas seleccionados basados en Internet con unos objetivos específicos en mente.

Las redes que corren mayores riesgos de ser atacadas son aquellas que cuentan con un número considerable de equipos públicamente accesibles. Tener muchos

puntos de acceso a una red multiplica el potencial para comprometer y gestionar estos riesgos se convierte en una tarea cada vez más difícil de realizar a medida que las redes crecen. Esto es conocido comúnmente como el dilema del defensor; un defensor debe garantizar la integridad de cada punto de acceso, considerando que un atacante solo necesita ganar acceso a través de uno para tener éxito.

Mitigar ataques

Uno de los principales objetivos, al menos de los más conocidos, de los administradores de seguridad de la información, es la de diseñar, probar e implementar medidas que contribuyan a mitigar los potenciales ataques que se produzcan a nuestra plataforma. Esto es así, aun cuando tomando una serie de medidas que consideremos las necesarias para enfrentar un potencial ataque, en medio de un ataque real, es cuando nos vamos a confrontar en la realidad de si resultaron efectivas o no las medidas que hemos tomado.

Además de confrontar este tipo de situaciones, y solucionar de manera permanente las vulnerabilidades, otra forma es enfocarse sobre los ataques y atacantes, es esta labor la que va a tomar la mayor parte del tiempo del administrador de seguridad, donde entran en acción sistemas que son particularmente emblemáticos y que son los que usualmente el común denominador de los usuarios, sean conocedores o no del área de la seguridad informática, asocian con esta área, los cortafuegos (del

inglés firewalls) y los localizadores de virus, cuya primordial razón de ser es obstaculizar la acción de posibles atacantes.

Al respecto, Bauer (2005, p. 53) nos dice: “Todavía no se ha diseñado ningún cortafuegos con cierta inteligencia sobre vulnerabilidades específicas de los hosts que protegen o de los valores que guardan, y no digamos de los antivirus. Sus únicas funciones son minimizar el número de ataques (en el caso de los cortafuegos, ataques basados en red; con los antivirus, ataques basados en software hostil) que suceden en sus intentos de llegar al objetivo”.

Los mecanismos de control de acceso, como pueden ser los esquemas de usuario/contraseña, fichas de autenticación y tarjetas, también están dentro de esta categoría, en el momento que su propósito es distinguir entre usuarios autorizados o no (potenciales atacantes).

Servicios de seguridad

Cualquier organización, independientemente de su tamaño, necesita de servicios de seguridad, normalmente las grandes organizaciones son las que usualmente caen en cuenta de esta necesidad y toman medidas para implementar soluciones de seguridad cada vez más complejas y a la vez costosas.

Tal como se ha venido comentando, con el crecimiento imparable de los sistemas de información, y el aumento de la exposición de los recursos de las organizaciones a potenciales intrusos o atacantes, la necesidad de contar con herramientas que ayuden a proteger los activos conforman una necesidad vital para la seguridad y el correcto funcionamiento de las organizaciones.

La arquitectura de seguridad OSI, mencionada por Stallings, W. (2004, p. 102) define el servicio de seguridad como: “Un servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización. Los servicios están diseñados para contrarrestar los ataques a la seguridad, ya hacen uso de uno o más mecanismos para proporcionar el servicio”.

En este mismo orden de ideas Stallings (2004, p. 102) establece que: “Los servicios de seguridad ameritan políticas y mecanismos de seguridad para su implementación.

Análisis simple de riesgos

El tema del análisis de riesgos pasa por la búsqueda de un modelo que busca establecer controles a partir de los resultados obtenido en el análisis previo. Expósito (2003, p. 60) señala: “El análisis de riesgos permite determinar cómo es, cuanto vale y como de protegidos se encuentran los activos. El análisis de riesgos proporciona

un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento".

Por otra parte, Mc Carthy y Campbell (2002, p. 42) definen el análisis y gestión de riesgos como: "El estudio para determinar las situaciones en que aparece un riesgo, los elementos que motivan dicha aparición y el alcance que puede tener el riesgo. Las tareas de análisis y gestión de riesgo no son un fin en sí mismas, sino que encajan en la actividad continua de gestión de la seguridad".

Una vez que se tienen identificados los activos electrónicos, vulnerabilidades, y los potenciales atacantes, se debe establecer una correlación y cuantificación. En muchos entornos, no es muy factible hacerlo por más que cuidemos los escenarios elegidos.

Al respecto dice Bauer (2005, p. 45): "Incluso un análisis de riesgo limitado puede ser de gran utilidad a la hora de justificar los costos de seguridad ante los directivos de una organización, o poner las cosas en perspectiva para el propio analista de seguridad de la información".

Una forma sencilla de cuantificar riesgos es calcular las expectativas de perdidas anualizadas, Bauer (2005, p. 46) establece que para cada vulnerabilidad, se calcula:

Expectativa de Pérdida Individual (costo) x Proporción Anual de Ocurrencias esperadas = Expectativas de Pérdidas Anualizadas (coste/año)

Tabla 1: Análisis simple de riesgo Modelo

Activo	Objetivo de Seguridad	Vulnerabilidad	SLE(euros/Incidente)	ARO(Incidentes/Año)
Puerta de enlace SMTP	Integridad del sistema	Bugs de sendmail	2.400	0,50
		Bugs de sistema	2.400	0,50
	Disponibilidad del sistema	Ataques DoS	950	0,50
Correos confidenciales (Información de los clientes)	Datos confidenciales	Capturas en Internet o ISP	50.000	2,00
		Compromiso del SMTP	50.000	2,00
		Intrusos Maliciosos	150.000	0,33
	Integridad de datos	Alteración al surcar Internet o ISP	10.000	0,25
		Compromiso del SMTP	10.000	0,50
		Correo falsificado	10.000	1,00
Correos no confidenciales (Información de las operaciones)	Integridad de datos	Alteración al surcar Internet o ISP	3.000	0,25
		Compromiso del SMTP	3.000	0,50

Fuente: (Bauer 2009)

Árboles de Ataque

Esta es una de las herramientas que puede servir también como alternativa para realizar un efectivo análisis de los riesgos en la seguridad de la información, ya que esta técnica es muy útil para modelar las diferentes formas que puede utilizar un atacante para alcanzar un objetivo.

Scheinner (1999, p. 55) explica al respecto lo siguiente: “Un árbol de ataque es simplemente una representación visual de los posibles ataques contra un determinado objetivo. El objetivo se denomina nodo raíz; los distintos pre objetivos para alcanzar al nodo raíz son los nodos hoja”.

Para construir un árbol de ataque el objetivo del atacante, tal como lo expresa Scheinner, se usa como raíz del árbol y, a partir de éste, de forma iterativa e incremental, se van detallando como ramas del árbol las diferentes formas de alcanzar dicho objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse.

Un ejemplo de esto puede ser el siguiente: un objetivo a atacar podría ser “robar los datos relacionados a las cuentas de clientes en una empresa transnacional”. Los medios para lograr esto directamente podrían ser los siguientes:

- Obtener las copias de seguridad del servidor de archivos de la empresa.
- Interceptar los correos electrónicos entre la empresa y sus clientes.
- Comprometer el servidor de archivos de la empresa desde cualquier parte mediante Internet.

Estos tres pre objetivos son los nodos hoja inmediatamente inferiores de nuestro nodo raíz.

Lo siguiente es determinar qué objetivos subyacentes consiguen cada nodo hoja. Éstos serían una siguiente capa de nodos hoja. Este paso se repetirá tantas veces como se quiera detallar y de la complejidad en la que se está analizando el ataque. La siguiente figura es un ejemplo de árbol de ataque.

Análisis del escenario

Según Cañizares (2012, p. 77): “Para poder elaborar un árbol de ataque hay que analizar el escenario al que nos enfrentamos y estudiar el problema desde el punto de vista del potencial atacante. Si se considera, que cuando un atacante se plantea el ataque a un objetivo elabora un plan, se debe ser capaz de analizar el escenario y determinar las posibles alternativas que estudiaría el intruso a la hora de elaborar dicho plan de ataque”.

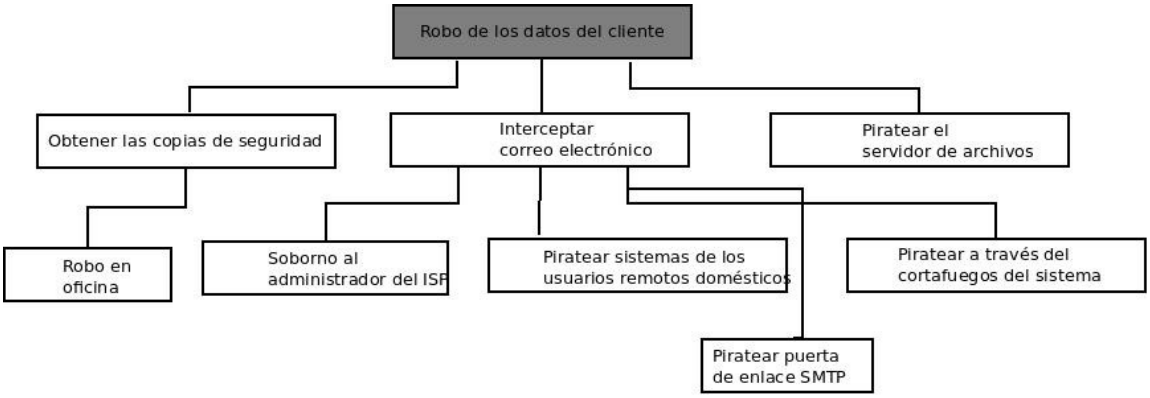

Figura 4: Un árbol de ataque de ejemplo. Fuente (Bauer: 2005)

Luego, Cañizares (2012, p. 78) establece las siguientes fases como parte de un plan de ataque:

- Fase 1: Obtención de información
- Fase 2: Determinación del objetivo estratégico
- Fase 3: Asignación de recursos
- Fase 4: Determinar los objetivos tácticos
- Fase 5: Elaboración de los planes tácticos
- Fase 6: Ejecución del ataque
- Fase 7: Análisis del resultado del ataque

Es importante destacar lo fundamental que resulta la información sobre las estructuras críticas que se encuentra disponible en fuentes abiertas. La elaboración de un árbol de ataque en pro de resguardar los activos de una organización permitirá tomar parte de las medidas necesarias para evitar los daños que pudiera ocasionar un incidente e seguridad en la plataforma.

Diseño de perímetros de red

Oppleman (2005, p. 115), ofrece la siguiente definición para un perímetro de red: “El perímetro de la red es la primera línea de defensa contra ataques y la combinación de amenazas procedentes de Internet”.

La manera en que se protege el perímetro ha cambiado radicalmente a lo largo de las últimas décadas. Las tecnologías de red y sus protocolos subyacentes han evolucionado y continúan evolucionando a un ritmo sin precedentes. Esta evolución ha hecho que muchas de las primeras tecnologías de seguridad del perímetro se hayan vuelto obsoletas, o por lo menos, de un valor limitado. Es importante tener esto en cuenta cuando se vayan a seleccionar soluciones de seguridad. Con respecto a este punto, Oppleman (2005, p. 116) dice: “Las siguientes tendencias han jugado un papel principal en la evolución de las tecnologías de seguridad del perímetro”:

- El concepto del perímetro tradicional de la red se ha difuminado: con la evolución de las redes privadas virtuales y de las tecnologías inalámbricas, el perímetro de hoy en día implica mucho más que el punto de acceso del proveedor de servicio. Además, con la difuminación del perímetro tradicional duro (hardware), se ha puesto más énfasis en la seguridad de los extremos de cara a defender el núcleo interno blando (software) de las redes actuales.

- Las velocidades de red continúan aumentado: En el momento de escribir este documento, no resulta extraña la conectividad en el escritorio a velocidades de gigabit y la velocidad no puede sino incrementarse en el futuro.

- Los protocolos se han vuelto mucho más complejos: Actualmente, existe toda una gama de protocolos encapsulados sobre HTTP, por ejemplo, lo que requiere reforzar las políticas de red a niveles cada vez más altos en la pila de protocolos.

Es importante acotar que los cortafuegos no son más que una pieza más de una aproximación multicapa que debe implementarse en toda organización que procure tener medidas de seguridad de la información básicas.

Arquitectura Interna contra externa

Cuando una organización conecta su red local a internet, deja abierto el acceso a todos los equipos de su red desde el exterior. La posibilidad de proteger los equipos

de forma individual, es particularmente compleja y no es óptima. En definitiva, para proteger a todos los equipos de una red, la solución debe ser global y enfocarse como un problema de red, aunque puedan establecerse mecanismos de protección de manera individual en cada uno de los equipos.

Una arquitectura de cortafuegos debería diseñarse y planificarse cuando se diseña la estructura de la red. Un cortafuegos no deja de ser un diseño de red en el que se emplean determinados componentes, cuya finalidad es la de canalizar el tráfico con los elementos apropiados y permitir o no según las reglas establecidas.

Bauer (2005, p. 59) establece: " La mayoría de las arquitecturas más comunes que tienden a verse hoy en día es la que puede verse en la figura N° 5, en esa figura, se muestra en primer término un enrutador con filtrado de paquetes, pero no como única línea de defensa. Directamente detrás se sitúa un cortafuegos. No hay conexión directa con Internet o desde el enrutador externo con la red interna; todo el tráfico que entra o sale pasa por el cortafuegos".

Definiciones de servicios de evaluación

En el área de Seguridad de la Información hay definidos un conjunto de servicios de evaluación conocidos con diversos nombres. La siguiente figura muestra las principales ofertas de servicios junto con la profundidad de evaluación que ofrecen y

su coste relativo. Cada tipo de servicio puede proporcionar distintos grados de evaluación de la seguridad.

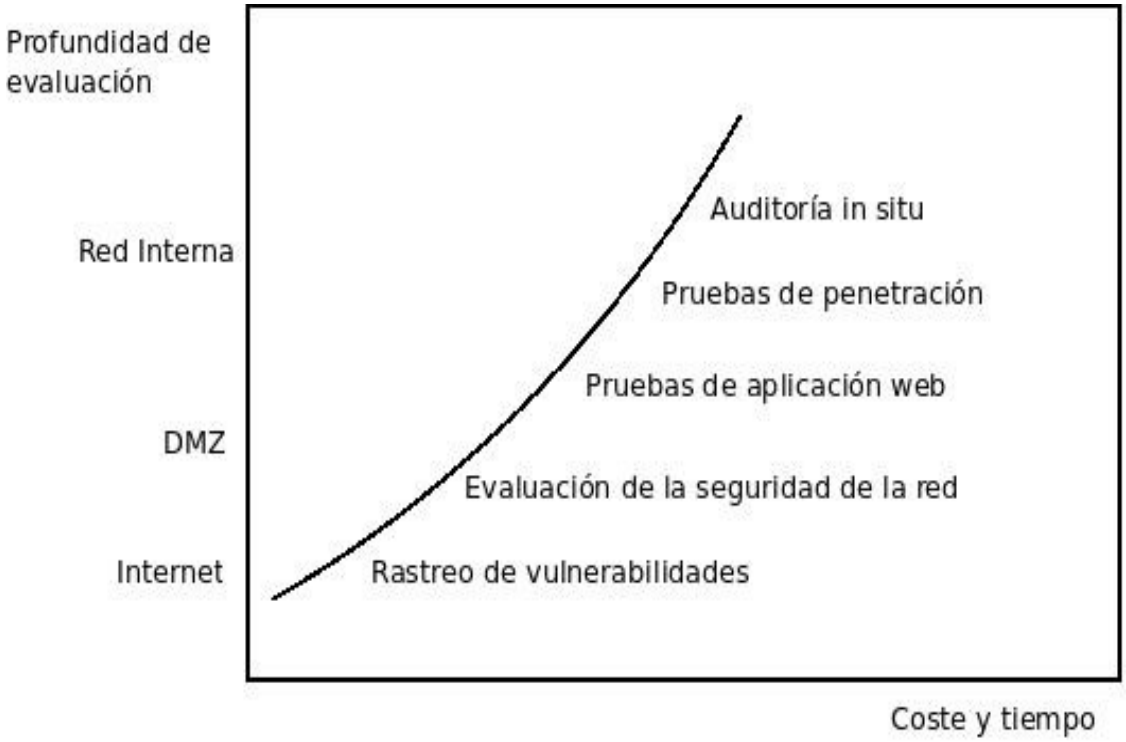

Figura 5: Distintos servicios de comprobación de la seguridad. Fuente (McNab 2008)

El rastreo de vulnerabilidades utiliza sistemas automatizados con los valores mínimos de calificación y evaluación de vulnerabilidades sobre el terreno. Es una forma de bajo costo de garantizar que no existan vulnerabilidades obvias, pero no proporcionan una estrategia clara para mejorar la seguridad.

La evaluación de la seguridad de redes es una mezcla eficaz de pruebas de vulnerabilidad con la cualificación. El informe final normalmente es un manuscrito, acertado y conciso, que proporciona consejos profesionales que permiten mejorar la seguridad de la organización.

La prueba de aplicaciones web involucra una evaluación de post-autenticación de componentes de aplicaciones Web, identifican diversas debilidades presentes en una aplicación Web dada. Probar este nivel implica una extensa cualificación manual e intervención del consultante, y no puede ser automatizada fácilmente.

Las pruebas de penetración puras tratan múltiples vectores de un ataque, para comprometer el entorno establecido como objetivo.

La auditoría in-situ proporciona la imagen más clara de la seguridad de redes. Los consultantes tienen acceso a los sistemas locales y ejecutan herramientas en cada sistema capaces de identificar algo inesperado, incluyendo programas dañinos, contraseñas de usuario vulnerables, accesos deficientes, y otros problemas.

McNab (2008, p. 38) establece que la mejor metodología de evaluación utilizada, tanto por un atacante decidido, como por consultores de seguridad, incluye cuatro componentes principales diferentes:

- Rastreo de la red para identificar redes IP y servidores de interés.

- Rastreo masivo de redes e investigación para identificar servidores potencialmente vulnerables.

- Investigación de vulnerabilidades y examen posterior de las redes, realizado a mano.

- Explotación de las vulnerabilidades y eludir los mecanismos de seguridad.

Adicionalmente complementa con lo siguiente: “Esta metodología completa es relevante para las redes basadas en Internet que sean examinadas de una forma “ciega”, con información limitada del objetivo (como un único nombre de dominio DNS). Si se solicita a un consultor que evalúe un bloque específico del espacio IP, se saltará la enumeración inicial de la red, comenzará con el rastreo masivo de la red y la investigación de vulnerabilidades” (p. 38).

Los servicios de evaluación de vulnerabilidades son una pieza fundamental en el mantenimiento cotidiano de la seguridad de la información, por cuanto nos permite establecer escenarios que pueden ser explotados por intrusos y de este modo tomar lo correctivos necesarios antes de que la ocurrencia tenga alguna consecuencia para la información de la organización.

Investigación de vulnerabilidades

Cada día se revelan nuevas vulnerabilidades en los servicios de red que se divulgan en la comunidad dedicada a la seguridad y en el mundo clandestino afín, utilizando para ello las cuentas de correo electrónico y los foros públicos de Internet.

Con frecuencia se publican herramientas de “prueba de concepto” para su uso por parte del personal de administración de seguridad de la información, mientras que la información sobre los verdaderos recursos para aprovechar los agujeros de seguridad es retenida por hackers éticos y no es revelada de manera pública.

McNab (2008, p. 187) establece que: “Con frecuencia se da el caso de que el rastreo masivo de la red no proporciona pistas detalladas de la configuración de servicios y de ciertas opciones activas, por lo que esta fase de la investigación conlleva un máster en pruebas manuales contra servidores clave”.

Tener conocimiento de las alertas de seguridad y la investigación permanente en este campo, proporciona un conocimiento y habilidades muy importantes al momento de realizar un diagnóstico mas o menos preciso del estado real de la red.

Monitoreo y Diagnóstico de redes

El monitoreo de redes surgió a partir de la necesidad de realizar diagnósticos efectivos para solventar problemas que pudieran presentarse en la actividad diaria de

las organizaciones y sus redes. Es importante monitorear la red y asegurarse de que el tráfico que es detectado pertenece efectivamente a equipos autorizados para generar el mencionado tráfico.

Los monitores de red, van un paso más allá de la simple identificación que nos ofrecen los utilitarios de sistema operativo, en cambio, un monitor de red es capaz de examinar la señalización y el tráfico que se produce en la red. Con el pasar del tiempo los monitores se han ido simplificando y ya no es preciso acumular una gran experiencia para su administración básica, se han hecho menos costosos y tienen una gran potencia.

Ford (1988, p. 553) dice: “La administración de red se refiere a cualquier arquitectura utilizada para administrar redes, Esta gestión es parte de la Arquitectura de Redes Abierta y se realiza de manera central a través de plataformas de administración. Se divide en cinco funciones que son similares a las funciones de administración de red especificadas en el modelo OSI *(Open System Interconection*)”.

Cualquier sistema protegido debe ir acompañado de logs detallados, completos y cuidadosos . Los logs tienen varios propósitos. Primero, ayudan a solventar todo tipo de problemas de sistema y aplicaciones. Segundo proporcionan señales de aviso antes de posibles abusos sobre el sistema. Tercero, después de producirse un

evento en el sistema o caída total, los log proporcionan datos cruciales que pueden ayudar a conocer en detalle la traza de lo acontecido.

Detección y Prevención de Intrusos

En una plataforma tecnológica con mecanismos de seguridad, todas las previsiones que se puedan tomar, sin entorpecer la operatividad de dicha plataforma, son adecuadas. En este contexto, hay un elemento que puede ser de ayuda invaluable para el personal de administración de seguridad y configurado de una manera adecuada es una poderosa herramienta para prevenir y actuar de manera proactiva ante potenciales riesgos para la integridad de la información de una organización. Se habla de los sistemas de detección de intrusos, conocidos como IDS, por sus siglas en inglés (*Intrusion Detection System*).

Los logs completos, pueden ser de ayuda para verificar el estado de la seguridad en un sistema, además de ser muy útiles al momento de una caída del sistema o un incidente de seguridad, pero esta herramienta solo va a registrar los eventos con mayor o menor detalle.

Un sistema de detección de intrusos, en palabras de Bauer (2005, p. 524): “Un servidor simple basado en IDS puede alertar de cambios inesperados en sistemas de archivos importantes basándose en los mecanismos de verificación de suma

almacenados” . En tanto una red IDS puede alertar de un ataque en potencia que se pueda estar produciendo, basándose en una base de datos de ataques conocidos o incluso basándose en las diferencias de estado de la red que considera fuera de estado normal. Algunos de estos ataques podrían pasar a través de un cortafuegos. Múltiples capas de seguridad son mejor que una.

A este respecto, Oppleman (2005, p. 169) comenta que: “Las tecnologías de detección y prevención de intrusiones pueden dividirse en varias categorías”. Se consideran en este trabajo las siguientes dos categorías:

- Detección de intrusiones basada en la red: Una visión general de los tipos fundamentales de tecnologías de detección de intrusiones basadas en la red. Hay que considerar aquí el potencial de ataques de inserción y evasión.

- Detección de intrusiones basada en la máquina: Una visión general de los mecanismos por los cuales funcionan los sistemas de detección de intrusiones basados en las máquinas.

Oppleman (2005, p. 163): “Aunque los cortafuegos están en constante evolución y son excelentes para proteger el perímetro en las capas de red y de transporte, se ha llevado a cabo un esfuerzo paralelo en la industria de la seguridad para identificar y alertar de los ataques. Nació toda una industria para identificar los ataques en las

redes. Nuevos dispositivos de seguridad y sistemas de detección de intrusiones llevaban a cabo su labor monitorizando un segmento de red y buscando signos conocidos (o previamente desconocidos) de un ataque".

Host IDS: Verificadores de integridad

Bauer (2005, p. 524): "Los hosts IDS dedicados tienden a contar con la comprobación de la integridad. En teoría, cuentan con una amplia categoría de herramientas. La comprobación de la integridad involucra la creación y mantenimiento de bases de datos protegidas de mecanismos de verificación de suma, criptografía mediante métodos hash y otros atributos de los archivo de sistema de un host crítico".

De esta manera, al menos en teoría, cualquier cambio inesperado puede ser el resultado de algún tipo de ataque y una adecuada configuración de la notificación de eventos puede alertar en etapas muy tempranas de un evento que debe ser atendido.

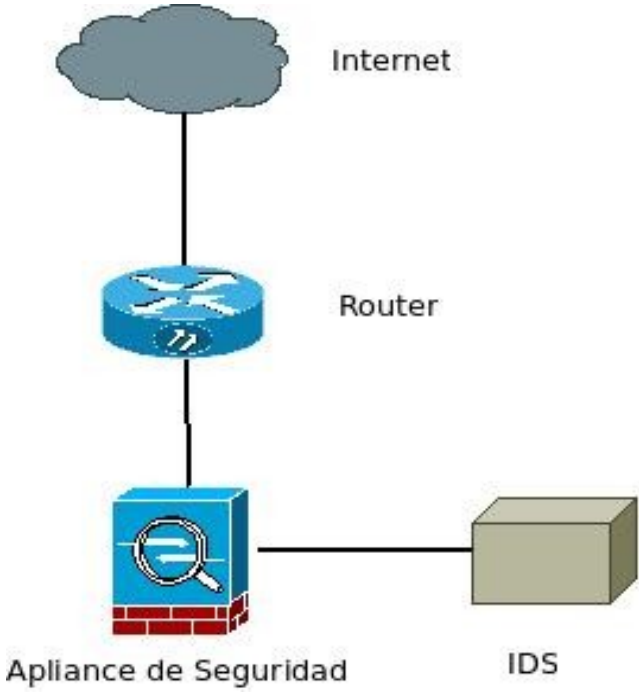

Figura 6: Esquema básico de red con Firewall e IDS Fuente: Elaboración propia

En este orden de ideas, mediante la comprobación regular de las utilidades del sistema y otros archivos importantes contra la base de datos de integridad, se puede minimizar la posibilidad de que algún servicio de nuestra plataforma sea comprometido sin nuestro conocimiento.

Es muy importante acotar aquí que cualquier comprobador de integridad con una base de datos no confiable es inútil. Es de imperiosa necesidad crear esta base de datos tan pronto como sea posible apenas se instale el sistema operativo en el host.

Para Oppleman (2005, p. 175): “Los Sistemas de detección y prevención basados en la máquina funcionan como software o agentes instalados en dispositivos finales. Normalmente se emplean para proteger servidores de aplicaciones críticos; sin embargo, pueden usarse fácilmente para proteger estaciones de trabajo”.

Las soluciones actuales proporcionan protección en varias capas del sistema operativo para frustrar los ataques que se originan tanto localmente como desde la red. Oppleman (2005, p. 179) menciona algunos de estos mecanismos:

- Prestaciones de cortafuegos de red para bloquear de forma predeterminada las conexiones entrantes.

- Prestaciones de prevención de intrusiones de red para bloquear ataques en las conexiones de red permitidas. Esta tecnología puede ser en principio muy similar a la usada en los sistemas de prevención de intrusiones basados en la red.

- Envolturas a llamadas al sistema operativo para poder añadir comprobaciones adicionales de seguridad a las mismas, y también aplicarles una política específica para cada aplicación. Este método se usa para imponer limitaciones a los recursos a los que puede acceder una aplicación, como, por ejemplo, los archivos, directorios y claves de registro.

Redes IDS: escanear firmas contra anomalías

Mientras que un IDS basado en máquina tiende a ser de un solo tipo (comprobadores de identidad), los IDS basados en red son de dos principalmente: los que se basan en los ataques firmados (patrones de tráfico característicos de ataques específicos) y los que poseen suficiente inteligencia para detectar un posible ataque en las variaciones de algunos conceptos del estado normal de la red). Usualmente se utilizan los basados en las búsquedas de firmas, pero muchos además acompañan cierto grado de control de anomalías de funcionamiento.

Bauer (2005, p. 527): “Hay varios tipos de sistemas basados en red, la mayoría caen dentro de la categoría que Marcus Ranum llama basados en auditoría, en lo que muchos de los datos obtenidos en los log no son analizados hasta que no ha sucedido el problema. En un sentido holístico, éste es un método muy potente, ya que implica la habilidad de construir firmas altamente sofisticadas por muy sutiles o complicados que sean los ataques”.

Como se puede notar, la compensación de los IDS basados en auditoría viene solo después que el sistema ha sufrido el ataque. Esto, en la mayoría de los casos es demasiado tarde.

Bauer (2005, p. 528) describe los dos principales tipos de IDS basados en red:

Sistemas basados en firma

Son los más comunes dentro de los IDS basados en red, por varias razones, en primer lugar, son muy simples: comparan las transacciones de la red con firmas conocidas de ataques y si una transacción dada coincide suficientemente con un ataque conocido, el IDS almacena una alerta en el log. Segundo, necesitan un mantenimiento bajo: todo lo que generalmente se necesita es mantener la base de datos de firmas actualizada. Tercero, tienden a registrar poco porcentaje de error.

Sistemas de detección de anomalías

Estos sistemas, que algunas veces también son denominados sistemas basados en estado, son mucho menos utilizados. Primero, tienden a ser complejos: determinar que constituye un funcionamiento “normal” del tráfico de la red es una tarea bastante compleja, por eso siguen cierto grado de inteligencia artificial para cualquier sistema automatizado que haga esto. Segundo necesitan un fuerte mantenimiento: incluso bien codificados y mecanismos de modelos estadísticos sofisticados, los IDS basados en estado normalmente requieren un largo y a veces dificultoso periodo de inicialización, durante el cual se recoge mucha información de los datos de red para crear una estadística que perfile el funcionamiento normal de la misma. El sistema requiere frecuentes y extensas parametrizaciones.

Para Bauer (2005, p. 530): “Los sistemas basados en detección de anomalías son los más próximos a futuras tecnologías IDS. Los sistemas basados en firma están limitados a ataques conocidos, especialmente a estos que su IDS tenga en la firma. Los sistemas basados en detección de anomalías son los únicos que pueden potencialmente detectar nuevos tipos de ataques”.

Detección de intrusiones basada en anomalías de protocolo

Los sistemas de detección de intrusiones basada en anomalías de protocolo funcionan buscando una actividad anormal o anómala sin el conocimiento de una vulnerabilidad específica. Para Oppleman (2005, p. 171) : “Los sistemas basados en anomalías de protocolo tienen la ventaja de entender el protocolo de la capa de aplicación subyacente que están examinando. Son capaces (en distinta medida) de procesar las opciones y campos individuales del protocolo y de evaluar el valor y el contenido de esos campos”.

Existen dos métodos principales que se emplean en los sistemas de anomalías de protocolo para identificar un ataque.

- Conformidad con el protocolo: La conformidad con el protocolo garantiza que un protocolo cumpla una especificación predefinida como la de un documento RFC

asociado. Aunque esto puede sonar eficaz, y en muchos casos lo es, no es extraño comprobar que los protocolos se desvían de sus estándares documentados.

- Análisis preventivo: El análisis preventivo implica la identificación de características anormales de una petición del protocolo antes de su aparición en un ataque. Este tipo de análisis preventivo puede ser útil en una situación en la que pueda surgir una amenaza de dia cero y el protocolo en cuestión se haya analizado previamente para identificar todos los posibles vectores de ataque.

Gestión de la información de la seguridad

Los sistemas de gestión de la información de seguridad surgieron como resultado del vasto volumen de información de seguridad que tenía su origen en los diversos sistemas de detección y prevención de intrusiones y cortafuegos. Oppleman (2005, p. 179) hace la siguiente aseveración: “Los sistemas de gestión de la información de seguridad sirven para normalizar, relacionar y proporcionar un contexto para los eventos que se producen en estos dispositivos. Interpretar el resultado de estos dispositivos no es una tarea pequeña, dadas las distintas capacidades de detección y las variaciones en la nomenclatura y en los formatos de salida”.

Las siguientes son las prestaciones que se puede considerar que son básicas para que un Sistema de Gestión de la Información de la Seguridad sea de utilidad:

- Normalización de eventos
- Correlación y reducción de eventos
- Correlación basada en reglas
- Correlación basada en campos
- Correlación de contexto
- Correlación de agregación y filtrado
- Correlación de comportamiento
- Correlación post-ocurrencia

En la siguiente tabla se puede observar una lista de comprobación sugerida para el desarrollo de defensas:

Tabla 2: Lista de comprobación para el desarrollo de defensas

Paso	Descripción
Recopilar sus necesidades	Antes de escoger una solución adecuada, es importante que defina sus necesidades. Determine si sus requisitos implican que necesita una solución basada en la red o en máquina. Si se trata de una solución basada en la red, ¿sólo le interesa la detección de ataques o también le interesa bloquearlos?
Construir una lista de candidatos	De acuerdo con sus necesidades, construya una lista de los potenciales fabricantes según sus ofertas. Tenga en cuenta la estabilidad y siga la pista del fabricante, ya que muchos se han agotado tratando de adquirir productos de fabricantes que ya no están en el mercado.
Evaluar a los candidatos	Es importante realizar una evaluación de los productos potenciales para determinar el más adecuado. Muchos fabricantes le proporcionarán plataformas de evaluación para simplificar esta tarea.
Desplegar su solución	Una vez adquirida, despliegue su solución tal y como recomiende su fabricante.

Fuente: Oppleman (2005)

Métricas

De acuerdo a Hyden (2010, p. 223), la medición es: “El acto de juicio o estimación de las calidades de algo, a través de la comparación con algo adicional”. En el campo de medición de elementos de la Seguridad de la Información, no son las métricas las que son sensibles en sí mismas, pues responden a hechos concretos sobre aspectos de la seguridad que requieren ser revisados, sino las mediciones que se derivan de ellas, es decir las valoraciones que se efectúan sobre las métricas las cuales son

juicios de valor humanos frente a referentes que deberán ser los más adecuados con la realidad de la empresa y su entorno competitivo.

Considerando lo anterior, Jaquith (2007, p. 112), confirma que si bien se establece un sistema de métricas basado en estándares como el ISO 27001 es un reto interesante, no es lo más adecuado dado que las mediciones asociadas con éste, estarán focalizadas en aspectos que son auditables y requerimientos de control, más que en la incorporación de las prácticas mismas; estará muy sesgada por criterios subjetivos de valoración, dado que se requiere definir qué y cómo, propios con la dinámica de la organización y sus estructuras de negocio, y finalmente, las métricas se enfrentarán al problema de la valoración, las cuales el mismo estándar no ofrece orientación al respecto.

En este mismo orden de ideas Brotby (2009, p. 229), establece: “Se mide para poder administrar”. Esto es, negociar un conjunto de recursos, acordar unos comportamientos requeridos y rendir cuentas. En conclusión para determinar la información necesaria para monitorear un proceso de seguridad se precisa dar respuesta a las siguientes preguntas:

- ¿Qué es lo que será administrado?
- ¿Cuáles son sus objetivos?

- ¿Qué decisiones se deben tomar?
- ¿Qué información es requerida para tomar dichas decisiones?
- ¿Qué procesos pueden proveer la información requerida?

Modelos

El Modelo es la representación de la estructura y manejo de la información de forma confiable, eficaz y oportuna, que facilita la toma de decisiones y da cuenta del estado de un ente en estudio en todas sus dimensiones.

Según Hurtado (2010, p.97): “Modelo hace referencia a lo deseado, a un ideal a lo perfecto o lo que debe ser. Así un modelo es la descripción sistemática, consciente y simplificada de una parte de la realidad, realizada mediante signos, símbolos, formas geométricas o gráficas y palabras”.

En este mismo orden de ideas, Bunge (Bunge, 1989; cp. Palella y Martins (2006)) da la siguiente definición: “Una representación idealizada de una clase de objetos reales”.

En proyectos de ingeniería y arquitectura es común desarrollar modelos antes de dar inicio a una construcción, ya que brinda múltiples ventajas:

- El modelo permite discutir con el cliente las necesidades a ser cubiertas.

- Sirve de base para definir la apariencia y el diseño del producto final.

- Permite representar y evaluar conceptos.

- Una vez finalizada la construcción, servirá de criterio de aceptación del producto, pues este no será aceptado a menos que se haya construido de acuerdo con las especificaciones que el modelo presenta.

En sistemas, la presentación de modelos cumple funciones similares, Fábregas (2008, p. 128) nos dice: “Un modelo permite representar una realidad compleja en términos simples, permite representar las características esenciales de un área funcional o un sistema y ayuda a plantear interrogantes cuya respuesta orientaran al planificador, al diseñador y al constructor del sistema”.

Modelos de datos y procesos

La mayoría de las metodologías que se usan hoy día trabajan en forma escalonada, para desarrollar sistemas de información: desde arriba hacia abajo, de lo general a lo particular, de los abstracto a lo concreto, de los resumido a lo detallado. Por esta razón, durante el desarrollo de un plan de TI o de un sistema de información, los ingenieros de sistemas estructuran una jerarquía de modelos que comienza con una

visión muy simple y general del sistema, continúan con pequeños modelos adicionales que van detallando en forma creciente.

Para Fábregas (2008, p. 130): “La elaboración de la jerarquía de modelos permite expresar en términos manejables la complejidad de los sistemas, por lo que se convierte en un excelente vehículo para trabajar inteligente y productivamente con los representantes funcionales en la definición de requerimientos”.

Modelos conceptuales de funcionamiento y físicos

Al desarrollar un sistema el analista va buscando respuesta a preguntas de concepto, de funcionamiento y de estructura:

- Las preguntas de concepto buscan dar respuesta a lo que hace el sistema que analizamos a lo que hará el sistema que estamos diseñando.

- Las preguntas de funcionamiento o utilización buscan dar respuesta a la forma como funciona el sistema actual o como va a funcionar el nuevo sistema.

- Las preguntas de estructura permitirán establecer cuáles son los componentes que conforman el sistema actual o que componentes deberán ser desarrollados para que el nuevo sistema funcione en la forma deseada.

Con el fin de dar respuesta a cada una de las preguntas en el transcurso de un proyecto de sistemas de información, se crean tres tipos diferentes de modelos Fábregas (2008, p. 132) los describe de la siguiente manera:

- Modelo conceptual o semántico, que muestra los procesos del negocio y la información que requieren (que hace o que hará el sistema).

- Modelo de funcionamiento o utilización, que muestra como operaran o funcionaran los procesos del negocio haciendo uso de los sistemas (como serán usados por los usuarios).

- Modelo físico, que muestra los componentes, sistemas, aplicaciones, módulos, bases de datos y la forma en que estos se organizan.

Modelo conceptual de datos

Es un modelo conceptual o semántico de datos, se describe el conjunto de datos acerca de los cuales un sistema maneja información. En otras palabras, el modelo conceptual de datos muestra, en forma gráfica, las cosas, eventos y hechos acerca de los cuales un sistema mantiene o mantendrá archivos o bases de datos.

En términos generales, un modelo de datos muestra:

- Registros y eventos acerca de los cuales el sistema maneja o almacena datos.

- Las asociaciones entre registros.

- Los atributos de cada uno de estos elementos, registros y sus asociaciones.

La estructura del modelo conceptual de datos no guarda ninguna relación con la forma en que se procesan o almacenan los datos, ya que este modelo centra su atención en el significado de los datos. (Fábregas, 2008, p. 133)

Modelo de utilización de los datos

Representa la forma en que el usuario agrupará y obtendrá acceso a los datos, es la visión que, de la base de datos del sistema, tiene el analista de sistemas, y constituye la materia prima para diseñar los archivos físicos o las bases de datos.

El modelo de utilización de los datos representa el conjunto de:

- Registro y tablas utilizadas para almacenar datos acerca de las entidades y asociaciones que componen el sistema.

- Vínculos entre estos registros y camino de acceso a los mismos.

- Datos contenidos en los registros.

- Claves y caminos de acceso a datos.

Si bien el concepto de un modelo de utilización de datos se deriva de un modelo conceptual de datos, su estructura debe adaptarse a las características del manejador de base de datos que será utilizado para desarrollar el sistema, con el fin de facilitar la tarea de diseño físico. (Fábregas, 2008, p. 134).

Modelo físico de datos

El modelo físico de datos representa la organización física de los datos en:

- Bases de datos y archivos integrados por registros que se almacenan juntos físicamente.

- Agrupación de registros en áreas de almacenamiento físicos, donde residirán físicamente los datos.

- Forma en que físicamente se almacenaran las interrelaciones entre registros.

El contenido del modelo físico de datos está dado por el contenido del modelo de utilización de los datos, igualmente su estructura está dada por la estructura de aquel modelo, pero también por las características del manejador de base de datos y de los medio disponibles para almacenar los datos. (Fábregas, 2008, p. 134).

Modelo conceptual de procesos

Así como el modelo conceptual de datos representa la comprensión de datos del sistema que se diseña, el modelo conceptual de procesos representa la esencia de los procesos y actividades que componen el sistema (que hace):

Un modelo conceptual de procesos representa:

- Procesos que se cumplen en el área de negocios.
- Actividades que se cumplen en cada proceso.
- Tareas que se cumplen en cada actividad.

Un modelo conceptual de procesos puede representarse con diagramas de descomposiciones funcional, incluyendo las definiciones de cada uno de los procesos, actividades y tareas. (Fábregas, 2008, p. 135).

Modelo de funcionamiento

Un modelo de funcionamiento representa la forma en cómo transcurre (o transcurrirá) la vida del negocio o la vida de los usuarios; se podría decir que representa un sistema “visto desde afuera del computador”.

- Forma en que influyen los datos de entrada y salida de los procesos.

- Actores o agentes externos que transmiten o reciben flujos de datos.

- Almacenamiento de datos que sirven como reservorios de datos del sistema.

Un modelo de funcionamiento a diferencia del modelo conceptual contiene indicaciones acerca de localización y forma de ejecutarse de cada una de las actividades que representan (manual o mecanizada, por lotes o por líneas, etc.) dicho en otros términos, el modelo de funcionamiento, además de incluir los procesos, las actividades y las tareas cumplidas en el sistema, también representan como serán ejecutadas o cómo funciona el sistema. (Fábregas, 2008, p. 135).

Modelo físico de procesos

Un modelo físico de procesos representa la estructura de sistema y la organización de sus componentes:

- Componentes: aplicaciones, programas, módulos, procedimiento.

- Organización de dichos componentes.

El contenido del modelo físico de procesos está dado por el contenido del módulo de funcionamiento e incluye todos los modelos de ejecución dentro del hardware y software disponible. (Fábregas, 2008, p. 135).

Modelos de Madurez

El desarrollo de Modelos de Madurez se ha dado con gran auge en muchos ámbitos tecnológicos y organizacionales. Ahora bien, según Sánchez y Cervera (2007, p. 107) “La madurez es la capacidad que tiene una organización de aprender y utilizar los conocimientos adquiridos para disminuir su desperdicio organizacional o incrementar su eficacia. La madurez organizacional se logra a través de la existencia de elementos capaces dentro de la organización, ya que no se puede contar con solo elementos que conocen del negocio, se requiere de personal capacitado en sistemas administrativos y tecnologías actualizadas para manejarlos de manera más eficiente”.

El modelo general sugerido por Sánchez y Cervera (2007, p. 107), presenta un análisis y descripción de un Sistema de Madurez, establece y permite medir 4 niveles de madurez organizacional, los cuales denotan una mayor capacidad progresiva de aprendizaje de la organización, y una capacidad de utilizar lo aprendido para elevar la eficacia y la calidad de los servicios que presta.

Estos niveles son los siguientes:

- Incipiente

- Reforzamiento
- Alto rendimiento
- Desarrollo sustentable

En estos cuatro niveles de madurez es posible ubicar cualquier organización, determinándose que aquellas que se encuentran en un mismo nivel de madurez presentan características similares en cuanto a su desempeño, así como en cuanto a sus fortalezas, oportunidades, debilidades y amenazas, lo que permite tipificarlas una vez analizadas.

La siguiente figura muestra las principales características de cada uno de los niveles de madurez propuestos por Sánchez y Cervera, se puede observar que existe una relación entre la menor madurez y menor eficiencia de la gestión.

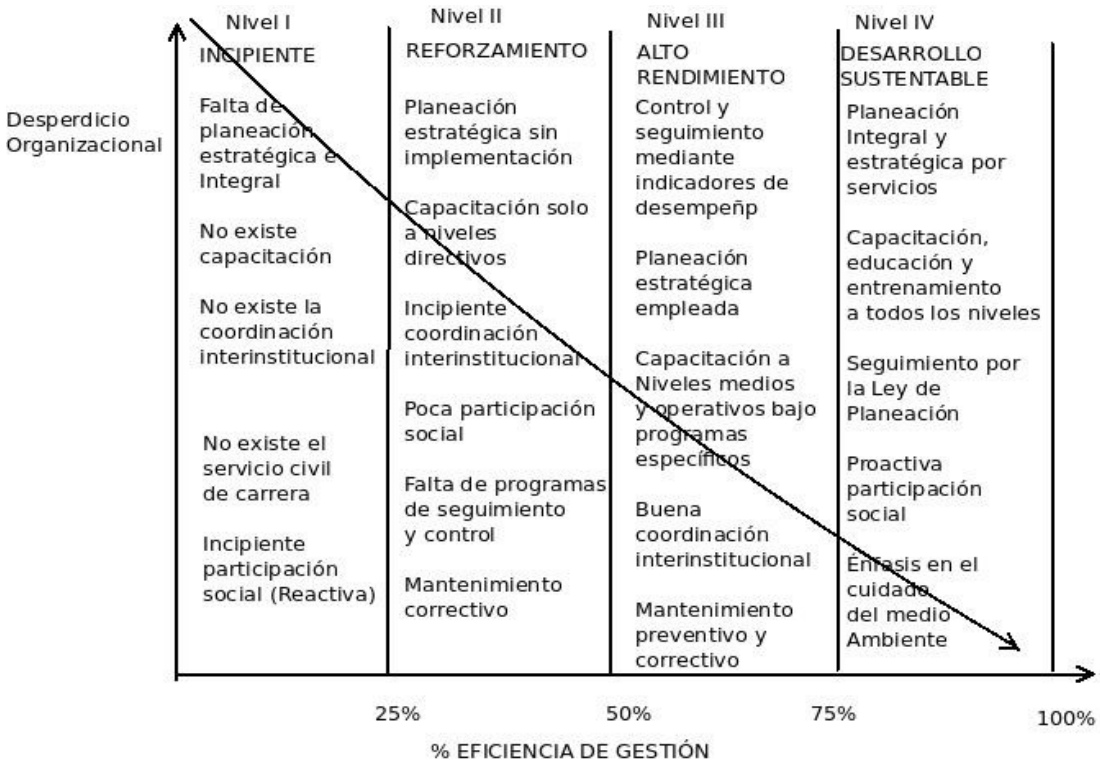

Figura 7: Modelo organizacional de Madurez. Fuente (Sánchez y Cervera: 2007)

En la definición del *Software Engineering Institute* (2016) un modelo de madurez "...contiene los elementos esenciales de procesos efectivos para una o más disciplinas y describe un camino de mejoramiento evolutivo desde procesos caóticos hasta procesos maduros con calidad y efectividad mejorada". Es decir, típicamente describe las mejores prácticas relacionadas a su ámbito de aplicación y apoya al mejoramiento de procesos gracias a que provee escalas evolutivas que describen caminos de mejoramiento.

Valdez (2010, p. 236) hace la siguiente aseveración: “Entonces, un enfoque multi-dimensional y holístico permite considerar como interactúan entre sí todos los elementos que son necesarios para que las iniciativas de e-government resulten exitosas y un enfoque evolutivo de madurez y capacidades permite describir cómo evolucionan todos los elementos considerados, apoyando el mejoramiento de procesos.

Adicionalmente el modelo debe estar acompañado de: una metodología que estandarice su aplicación, para que las mediciones y evaluaciones sean rigurosas y replicables, y de la institucionalidad gubernamental adecuada para que sea posible llevarlas a cabo efectivamente”.

Estado del Arte

Los modelos estudiados pueden categorizarse en cinco (5) grupos, como se puede ver en la Fig. 10, cada grupo presenta elementos, conceptos y enfoques que pueden ser considerados, reusados y adaptados a los requisitos del modelo a construir.

Modelos Clásicos de Madurez y Capacidad

Replicados por muchos otros modelos en diversos ámbitos tecnológicos y organizacionales, analizaron porque proveen la estructura típica de un modelo de madurez y capacidad. En este grupo se destaca el de Integración de Modelos de

Madurez de Capacidades CMMI (enfoque estadounidense) e ISO/IEC 15504 (enfoque europeo).

Modelos Gubernamentales

Desarrollados por gobiernos, consultoras y académicos para ayudar a las agencias gubernamentales a identificar y mejorar sus niveles de madurez en relación ***al e-government***. Es destacable la experiencia australiana y canadiense; AGIF incluye a BPIF (*Bussines Procces Interoperability Framework*), el cual contiene un modelo de madurez que puede ser usado por las agencias para identificar su nivel actual de madurez de interoprabilidad a nivel de negocio.

Modelos de Enfoque Holístico para Proyectos e-Government

Están diseñados para ser aplicados en proyectos de desarrollo de servicios públicos electrónicos. Un modelo bien conocido en la comunidad académica de e-government es el Framework Holístico de Wimmer, su propósito es apoyar el modelamiento integrado de servicios públicos y su sincronización con los desarrollos tecnológicos, para que el servicio electrónico resultante del proyecto satisfaga todos los requerimientos relevantes.

Modelos de evolución de e-Government

La evolución del e-Government es comúnmente modelada por etapas secuenciales, así por ejemplo el Banco Mundial afirma que se siguen las mismas etapas que en el e-commerce.

Existen otros Modelos organizacionales de madurez, que se describe a continuación:

Modelo de Nolan

El modelo de Richar Nolan describe las fases de asimilación tecnológica por la que pasa una empresa, al enfrentarse al reto de implementar una nueva tecnología. En realidad, Nolan presenta dos modelos, uno en el que se describen cuatros fases de asimilación y otro de seis fases. Es por esto que Nolan (1979, p. 88) explica el modelo de las cuatro fases que considera que las empresas tienen una cartera de tecnologías de la información diferentes, donde cada tecnología pasa a través de las siguientes fases:

- Fase uno: denominada Iniciación, se caracteriza por ser una etapa de introducción, aprendizaje y escaso control o planificación.

- Fase dos: lleva por título Expansión o Contagio, en esta los potenciales usuarios se sienten entusiasmados por las posibilidades de la nueva tecnología y sus aplicaciones. La experimentación y los gastos crecen aceleradamente, aparece la planificación y el control.

- Fase tres: titulada como Formalización o control, en esta surgen controles que frenan el crecimiento de los presupuestos en función de la adopción de las tecnologías, así como del número de aplicaciones a desarrollar, se exige calidad.

- Fase cuatro: llamada Madurez esta consigue la integración orgánica de las aplicaciones así como la planificación y control forman parte de las necesidades de la empresa, y las Tecnologías de la Información estén alineadas con los objetivos de la misma.

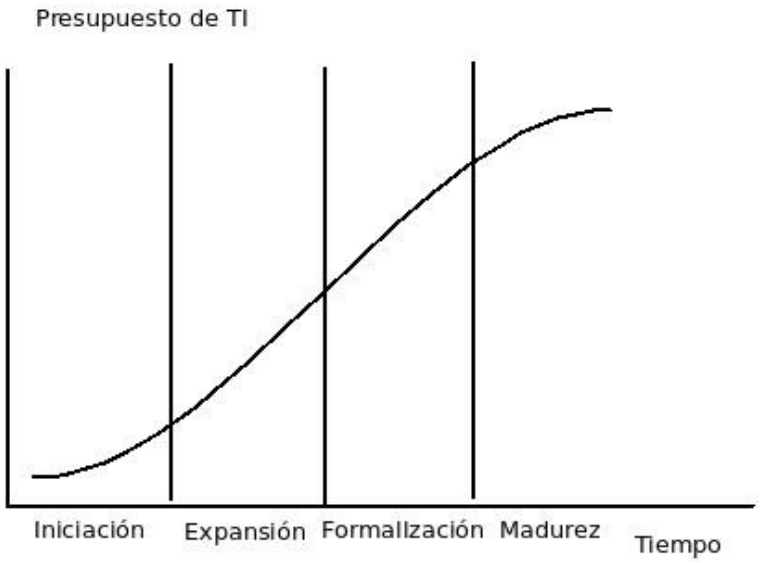

Figura 8: Modelo de Nolan (4 etapas). Fuente (Nolan: 1979)

En este mismo orden de ideas, el segundo modelo consta de seis fases y Estay-Nicular, C. (2006, p. 101) las describe como sigue:

- La primera fase es Inicio, es donde pocos individuos en la empresa aceptan aplicar la nueva tecnología para reemplazar los viejos métodos probados, ya que dichos métodos resultan conocidos y cómodos aunque también pueden ser poco eficientes o sujetos a mejoras.

- La segunda fase es Contagio, los beneficios de la nueva tecnología se hacen evidentes y todos en la empresa desean utilizarla, lo que trae como consecuencia una proliferación muchas veces exagerada y anárquica de la nueva y ahora

ampliamente aceptada tecnología. Nolan la denomina como snack, combinación de falta de control y abundancia de recursos.

- La tercera fase es Control, como su nombre lo indica controla o administra el uso y los riesgos de la nueva tecnología mediante normatividad y políticas institucionales, entre otros medios.

- La cuarta fase es Integración, en la cual se logran consolidar los beneficios sinérgicos y repetitivos de dicha integración.

- La quinta fase es la de Datos, en la cual la organización se orienta en consolidar una base de información o de conocimientos que contenga todo el conocimiento de la organización en forma integrada, no redundante y reutilizable.

- La sexta fase es la de Madurez, en la cual la organización logra obtener un portafolio de aplicaciones integrado y completo que soporta los objetivos institucionales y permite un aprovechamiento óptimo de la tecnología.

En la siguiente figura podemos ver de manera gráfica lo anteriormente expuesto.

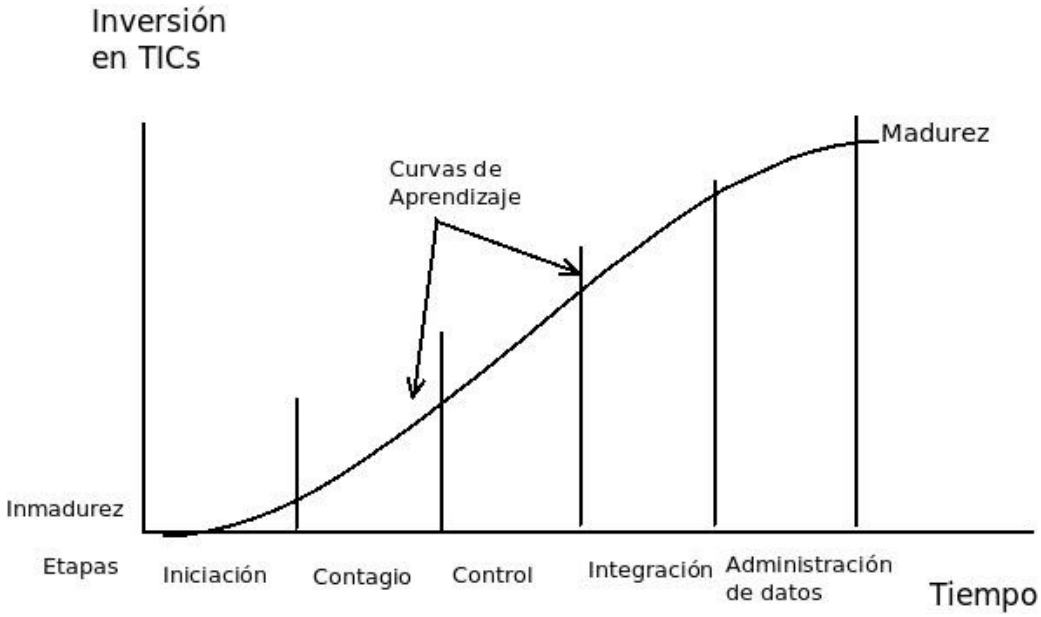

Figura 9: Modelo de Nolan (6 etapas) Fuente (Estay Niculcar: 2006)

El Modelo de Madurez de la Seguridad (MMS)

El objetivo de este modelo es servir de ayuda a las organizaciones para comprender su estado actual en mantenimiento de la Seguridad de la Información. Fue ideado por Vicente Aceituno, y según sus palabras: “Nos proporciona un método para alcanzar el grado de madurez óptimo para la organización”.

El modelo consta de cinco niveles, y según Aceituno (2004, p. 128): “Este estándar esta mas orientado a cumplir los objetivos del negocio”.

Este estándar se basa y es compatible con otros estándares tales como:

- ISO9001 (Sistema de Gestión de la Calidad)
- ISO27001 (Sistema de Gestión de Seguridad de la Información)
- ITIL (Biblioteca de Infraestructura de Tecnologías de la Información)
- CoBIT (Objetivos de Control para la Información y tecnologías relacionadas)

Los cinco niveles son descritos de la siguiente manera:

- Inicio, la seguridad no está reconocida como una característica deseable de la organización.
- Reconocimiento, la seguridad ya es reconocida como característica deseable de la organización. Las responsabilidades de la seguridad de la información no están definidas. Por lo tanto, no existe un departamento de seguridad.
- Definición, la seguridad es reconocida, la presencia de incidentes de seguridad no suele conducir a máximo impacto y las responsabilidades y funciones de la seguridad están definida, además existe una normativa.

- Gestión, la ausencia de incidentes de seguridad es una consecuencia de los esfuerzos permanente de la organización para prevenirlos y afrontarlos. Cabe destacar, la presencia de estos casi nunca conduce a un máximo impacto económico y negativo en los servicios. Existe un Plan de Continuidad de Operaciones que considera el estado de la organización en caso de ocurrir un incidente. Se evalúan constantemente los incidentes, activos, las soluciones, vulnerabilidades. En resumen, se realiza un Análisis y Gestión de la Seguridad.

- Óptimo, existe y se aplica una política de seguridad y se realiza un Análisis y Gestión de Riesgo.

Modelo de Madurez para la Administración y el Control de Procesos de TI (CoBIT)

Está basado en un método de evaluación de la organización, de manera tal que pueda ser evaluada desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque es derivado del modelo de madurez del *Software Engineering Institute* que definió para la capacidad de desarrollo del software. Los niveles de madurez están diseñados como perfiles de los procesos de TI que una organización reconocería como descripciones de posibles estados actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan

los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la administración podrá identificar:

- El desempeño real de la empresa- Donde se encuentra la empresa hoy
- El estatus actual de la industria- La comparación
- El objetivo de mejora de la empresa- Donde desea estar la empresa

El modelo de Madurez para la Administración y el Control de los Procesos de TI (COBIT) está compuesto por seis niveles, los cuales se detallan a continuación:

- 0 No existente: carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
- 1 Inicial: existe evidencia que la empresa ha reconocido de que los problemas existen y requieren ser resueltos. Sin embargo, no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o por cada caso. El enfoque general hacia la administración es desorganizado.
- 2 Repetible: se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los

procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y por lo tanto los errores son muy probables.

- 3 Definido: los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

- 4 Administrado: es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

- 5 Optimizado: los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Figura 10: Modelo para la administración y el control de los procesos de TI (COBIT) Fuente (IT Governance Institute: 2005)

La gestión del conocimiento

No existe en la literatura una sola definición de gerencia del conocimiento. Al respecto, Urbaez (2005, p. 344) la define como el proceso sistémico y específico de una organización, cuya finalidad es adquirir, organizar y comunicar tanto el conocimiento tácito como el explícito de los empleados, para que otros empleados puedan hacer uso de él y así ser más productivos en su trabajo. Estos autores consideran que el conocimiento tiene poco valor para la organización si no se comparte y la habilidad para integrar y aplicar el conocimiento especializado es fundamental para que una organización sea capaz de crear y mantener ventajas competitivas.

Por su parte, Zorilla (1997, p. 47) la define como el proceso de administrar continuamente conocimiento de todo tipo para satisfacer necesidades presentes y futuras e identificar y explotar conocimientos, tanto existentes como adquiridos que permitan el desarrollo de nuevas oportunidades. Estos planteamientos manifiestan en parte, tal y como lo manifiestan Escorsa et al (2000, p. 100) que la gerencia del conocimiento se orienta en la práctica hacia la clasificación de los diferentes conocimientos que los empleados de la empresa han acumulado de forma que puedan ser compartidos. Otras definiciones se orientan a relacionar la gerencia del conocimiento con la captación y uso del conocimiento de los individuos para que esté disponible como recurso organizativo independiente, Gottschalk, (2003, p. 112).

Seaton y Bresó (2001), citados por Klarson (1999) y Tiwana (2000) plantean que las distintas definiciones de gerencia del conocimiento pueden agruparse en dos enfoques: el que destaca su contribución a los procesos de aprendizaje y desarrollo organizacional y el que destaca su importancia en función de su potencial para la generación de recursos económicos. La versión organizacional establece que el único recurso realmente competitivo de la empresa es el conocimiento; y considera que la primordial tarea de la misma debe ser la sistematización de los procesos mediante los cuales sus empleados adquieren y generan los conocimientos necesarios para responder a los retos presentes, anticiparse a los retos futuros y

adaptarse para enfrentar oportunidades o amenazas que resulten de la interpretación de las fuerzas que definen sus escenarios de actuación.

Entre los autores que sostienen el enfoque económico o rentable de la gerencia del conocimiento se encuentran Bukowitz y Williams (1999, p. 67), Klarson (1999) y Tiwana (2000) (citados por Seaton y Bresó, 2001). Los primeros la definen como el proceso mediante el cual las organizaciones generan riquezas a partir de sus activos intelectuales o de conocimientos. Klarson por su parte considera que la gerencia del conocimiento es la habilidad para crear y retener mayor valor a partir de pericias medulares de la organización; y Tiwana establece que la gerencia del conocimiento es el proceso de utilización del conocimiento organizacional en la creación de valor y generación de ventajas competitivas.

Generación de conocimientos

La generación de conocimientos requeridos puede resultar interesante cuando la institución posee algún tipo de conocimientos de manera exclusiva, o estos son relativos a competencias esenciales de la organización. Aunque una de las principales razones por las que pueden interesar esta opción es la carencia de éstos fuera de la organización o la inviabilidad de adquirirlos por razones de costos.

El control y mejora del proceso consiste en formalizar el conocimiento utilizado para la solución de problemas para, posteriormente, poder realizar mejoras del proceso. Este tipo de actividad, descrito por Pazos (2006, p. 82), comprende cuatro niveles:

- Nivel del dominio. En este nivel se define el dominio en base a conceptos, relaciones y atributos. Esto también puede servir para establecer el marco de referencia común.

- Nivel de tarea. Consiste en un nivel de formalización y, o, protocolización de las tareas realizadas en la institución.

- Nivel estratégico. Comprende el control y monitorización de la solución de problemas.

- Nivel de inferencia. En este nivel se catalogan métodos de solución de problemas genéricos y se definen la forma de las inferencias para solucionar nuevos problemas.

El uso de las Tecnologías de Información y la Gestión del Conocimiento

En la actualidad el hecho de reconocer que los conocimientos son un activo de vital importancia dentro de las instituciones, teniendo una clara influencia dentro de su efectividad, ha desencadenado el interés por enfoques de las actividades básicas de

la Gestión del Conocimiento. Tradicionalmente, los organizaciones han tratado la Gestión del Conocimiento bien desde un punto de vista general o desde otro meramente tecnológico, más específico.

Hoy en día se cuenta con un conjunto de herramientas y tecnologías de la información ideales para el desarrollo de Gestión del Conocimiento. Sin embargo, Pazos (2007, p. 94), realiza la siguiente advertencia en torno a este tema: “Es importante recordar, que la tecnología no hace la solución y que los sistemas finales no sólo están formados por máquinas, software, etc., sino que deben tener un alto componente de integración con procedimientos, trabajadores expertos, directivos, usuarios, incluso los beneficiarios finales o público consumidor de los productos que se generen, etc.

Dentro de esta tecnología se pueden incluir desde los hoy día muy comunes portales, hasta los grandes sistemas que intentan dar soporte a la iniciativa de Gestión del Conocimiento en su totalidad, capturando y haciendo disponible el conocimiento institucional, como las Memorias Institucionales, pasando por Sistemas de Bases de Conocimiento, groupware, Agentes Inteligentes, proceso de minería de datos, etc”.

Gobierno TI

Aunque no existe una única y universalmente adoptada definición de Gobierno TI sí existe un consenso general sobre la importancia de disponer de un marco general de referencia para la dirección, administración y control de las infraestructuras y servicios de TI. (Ostiasis, 2011, p. 48).

Para aclarar las diferencias quizás los más conveniente sea tomar un ejemplo que se aparta del entorno de las Tecnologías de Información y que forma parte de la cotidianidad: Gobierno vs Administración Pública.

Según Ostiasis (2011, p. 49): “El gobierno es el responsable de establecer políticas y directrices de actuación que recojan las inquietudes y cubran las necesidades de los ciudadanos. Las administraciones públicas son las encargadas de asegurar que esas políticas se implementen, ofreciendo los servicios correspondientes, asegurando el cumplimiento de las normas establecidas, prestando apoyo, recogiendo reclamaciones y propuestas, etc.

Es evidente la dificultad de establecer un conjunto de buenas prácticas para el buen gobierno, sin embargo, estas existen de hecho y ejemplo de ello son la Declaración Universal de Derechos Humanos y todo el corpus de derecho internacional.

El Gobierno TI es parte del Gobierno Corporativo y como tal debe centrarse en las implicaciones que los servicios e infraestructura TI tienen en el futuro y sostenibilidad de la empresa asegurando su alineación con los objetivos estratégicos.

La creciente importancia de los servicios TI para las empresas hace pensar que todos los aspectos relacionados con el Gobierno TI serán un tópico alto en los próximos años y que se realizarán importantes desarrollos en ese terreno.

Administración Pública

Según Parra Manzano (2005, p. 76):

"Es un término de límites imprecisos que define al conjunto de organizaciones estatales que realizan la función administrativa del Estado. Por su función, la Administración Pública pone en contacto directo a la ciudadanía con el poder político, satisfaciendo los intereses públicos de forma inmediata, por contraste con los poderes legislativo y judicial que los hacen de forma mediata".

Principalmente lo integran el Poder Ejecutivo y los organismos que dependen de éste. Por excepción, algunas dependencias del poder ejecutivo no integran la noción de "Administración Pública" en los otros dos poderes o en organismos estatales que no dependan de ninguno.

La noción alcanza a los maestros y demás trabajadores de la educación pública, así como a los profesionales de los centros de salud estatal, a las policías y a las fuerzas armadas. Se discute, sin embargo, si la integran los servicios públicos prestados por organizaciones privadas por habilitación del Estado. El concepto no alcanza a las entidades estatales que realizan la función legislativa ni la función judicial del Estado.

Estructura de la Administración Pública en Venezuela

De acuerdo a Parra Manzano (2005, p. 78) los siguientes son los niveles de la Administración Pública Nacional:

Se rige por las disposiciones de la Ley Orgánica de la Administración Pública (LOAP), esta Ley creada con la finalidad de ampliar y organizar la Administración del Estado atendiendo a la organización y competencia de los poderes públicos, establecidos en la Constitución de forma descentralizada, regulando políticas administrativas y estableciendo normas básicas sobre los archivos y registros públicos.

La Administración Pública es una organización que está conformada por las personas jurídicas estatales (entes) y por sus órganos, como lo precisa la Ley Orgánica de la Administración Pública en su Artículo 115.

Administración Pública Central

Según el Artículo 45 de la Ley Orgánica de la Administración Pública son órganos superiores de dirección de la Administración Pública Central, El Presidente o Presidenta de la República, el Vicepresidente Ejecutivo o la Vicepresidenta Ejecutiva, el Consejo de Ministros, los ministros o ministras y los vice ministros o vice ministras.

Son órganos superiores de consulta de la Administración Pública Central, La Procuraduría General de la República, El Consejo de Estado, El Consejo de Defensa de la Nación, los gabinetes sectoriales y los gabinetes ministeriales.

El Presidente de la República

El poder ejecutivo reside en el presidente el cual tiene entre sus funciones administrativas, el manejo de la Haciendo Pública Nacional: Decretar créditos adicionales, previa autorización de la Asamblea Nacional, negociar empréstitos nacionales, celebrar contratos de interés nacional, designar el procurador, fijar el número de ministros entre otros.

Los Ministros y Viceministros

Según el Artículo 242 de la Constitución de la República Bolívariana de Venezuela (CRBV), los Ministros son órganos directos del Presidente, reunidos conjuntamente con el Vicepresidente forman el Consejo de Ministros, son responsables de sus

propias resoluciones solidariamente, es decir, que ningún ministro puede escudarse en los demás, sus actuaciones se rigen por la Ley Orgánica de la Administración Central (LOAC).

El manejo de los recursos en los ministerios viene de la cuota que se le asigna del total del Presupuesto Nacional, consta de dos etapas, la primera de la formulación y la segunda que es la ejecución. La cual distribuyen a sus dependencias por medio de Órdenes de Pago, que le son depositadas en una entidad financiera del Estado.

A partir del año 2006 la formulación y ejecución del presupuesto en los ministerios se está realizando por la elaboración de proyectos, solo los proyectos aprobados son los que recibirán recursos.

Administración Descentralizada

La descentralización de la Administración Pública se desarrolla atendiendo al principio de simplicidad en los trámites administrativos, para ello se creó la Ley de Simplificación de Trámites Administrativos (LSTA) de 1999, se destinó específicamente a desarrollar, en detalle el principio de simplificación con el objeto de racionalizar las tramitaciones que realizan los particulares ante la Administración Pública, para mejorar su eficiencia, utilidad y celeridad, así como reducir sus gastos operativos.

Artículo 30 de la Ley Orgánica de la Administración Pública (LOAP) " Con el principio de profundizar la democracia y de incrementar la eficiencia y la eficacia de la gestión de la Administración Pública, se podrán descentralizar competencias y servicios públicos de la República a los estados y municipios, y de los estados y municipios, de conformidad con la Constitución de la República Bolívariana de Venezuela y la Ley.

Entes de la Descentralización Funcional

Está clasificada en Institutos Autónomos, Empresas del Estado, Empresas Matrices, Fundaciones del Estado y asociaciones y sociedades civiles del Estado.

Institutos Autónomos

Son organismos oficiales con personalidad jurídica, financiados por el Estado, esta figura se crea con la finalidad de que su desempeño sea más ágil a la hora de brindar soluciones, sin tener que recurrir a un nivel central. (no dependen de las decisiones de Ministros o Consejos de Ministros).

Debido a que el manejo de los recursos también gozan de autonomía, están sujetos a rendir cuentas a la Contraloría General de la República.

Su creación es por medio de la Ley desde la Constitución de 1961 y está a cargo del Poder Legislativo.

Empresas del Estado

Artículo 100 de la LOAP: “Son empresas del Estado las sociedades mercantiles en las cuales la República, los estados, los distritos metropolitanos y los municipios o alguno de los entes descentralizados funcionalmente a los que se refiere esta Ley, solos o conjuntamente, tengan una participación mayor al cincuenta por ciento del capital social.

Empresas Matrices

Según el Artículo 105 de la LOAP, se refiere la operación a la vinculación existente de varias empresas del Estado en un mismo sector y estas pueden ser creadas, por el Presidente, por los Gobernadores o Alcaldes.

Fundaciones del Estado

Según el Artículo 108 de la LOAP, Son llamadas fundaciones a los organismos que funcionan con patrimonio del Estado (mayor al 50%), que se les considera de utilidad pública, por su carácter artístico, científico o literario, por ejemplo el Centro Simón Bolívar (CSB).

Asociaciones o Sociedades Civiles del Estado

Según la LOAP, en este caso la participación del Estado es en carácter de Socio o miembro con un aporte del cincuenta por ciento o más del capital , deberán ser

autorizadas por el Presidente o Presidenta de la República, mediante decreto o a través de resolución dictada por máximo jerarca descentralizado funcionalmente.

Administración Pública Estatal

Los Estados son entidades autónomas, con personalidad jurídica plena, obligadas a mantener la independencia, soberanía e integridad nacional y a cumplir la Constitución de la República, esta autonomía política, administrativa, jurídica y tributaria, tienen sus límites en la Constitución, en cuanto al ejercicio de competencias.

De acuerdo al Artículo 160 de la CNRBV la administración de los Estados corresponde a los gobernadores, su gestión será vigilada por el Contralor del Estado, las funciones legislativas estarán a cargo del Consejo Legislativo, los Consejos de Planificación y Coordinación de Políticas Públicas actuarán para coordinar las políticas de descentralización.

Administración Pública de los Distritos Metropolitanos

Los distritos metropolitanos surgen cuando dos o más municipios desean unirse ya sea para compartir la misma actividad económica, social o física, pueden ser de una misma entidad federal o distinta, lo cual será evaluado por la Asamblea Nacional,

ejemplo de esto es el Distrito Metropolitano de Caracas, formado por el Estado Miranda y el Distrito Capital.

La administración de los Distritos Metropolitanos se realizará atendiendo a las condiciones poblacionales, desarrollo económico y social, según el Artículo 172 de la CRBV, las competencias metropolitanas serán asumidas por los órganos de gobierno respectivo distrito metropolitano.

Administración Pública de los Municipios

La administración de los municipios corresponde al Alcalde, el control y vigilancia de los ingresos y gastos corresponde al Contralor Municipal, los cuales gozan de autonomía orgánica según la Ley Orgánica de Régimen Municipal, el poder legislativo, corresponde al consejo integrado por los concejales.

Marco Organizacional

Marco de Interoperabilidad de Venezuela

En la página del Ministerio del Poder Popular para Ciencia, Tecnología e Innovación con respecto al Marco de Interoperabilidad se puede leer lo siguiente: “El Marco de Interoperabilidad para el Estado venezolano constituye un logro significativo en la transformación tecnológica, el MIO como también se conoce es un documento de referencia para la creación, desarrollo e implementación de forma efectiva de la

Interoperabilidad, con el fin de agilizar los trámites y prestar un mejor servicio a la ciudadanía, estructurado en cinco capítulos que incluye las bases legales, conceptos de Interorabilidad (IO), políticas de implementación, estándares y recomendaciones generales para la aplicación de la IO en procesos interinstitucionales".

En este mismo orden de ideas, se puede obtener la siguiente información, asociada a este marco, "La interoperabilidad (IO) es la capacidad que tiene el Estado para que sus organismos y demás entes intercambien datos entre sí, a través del uso de Tecnologías de Información".

Es así, como se debe tomar en consideración que diversos organismos de la Administración Pública Nacional han mantenido reuniones que procuran integrar en una plataforma común los procesos correspondientes a cada una de dichas instituciones, entre las cuales tenemos:

- Vicepresidencia de la República
- Ministerio del Poder Popular de Planificación y Finanzas
- Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres
- Comisión de Administración de Divisas

- Compañía Anónima Nacional Teléfonos de Venezuela
- Oficina Nacional de Contabilidad Pública
- Servicio Administrativo de Identificación, Migración y Extranjería
- Servicio Nacional Integrado de Administración Aduanera y Tributaria
- Servicio Nacional de Contrataciones
- Superintendencia de Servicios de Certificación Electrónica
- Instituto Venezolanos de los Seguros Sociales

Es importante acotar que en el proceso de investigación llevado a cabo para el desarrollo del presente documento, se realizaron consultas en torno al tema de Seguridad de la Información para el desarrollo del Marco de Interoperabilidad y se aplicaron los instrumentos desarrollados, a personal responsable de la Seguridad Informática de todos los entes antes mencionados

Historia del IVSS

El 9 de octubre de 1944, se iniciaron las labores del Seguro Social, con la puesta en funcionamiento de los servicios para la cobertura de riesgos de enfermedades,

maternidad, accidentes y patologías por accidentes, según lo establecido en el Reglamento General de la ley del Seguro Social Obligatorio, del 19 de febrero de 1944. En 1946 se reformula esta Ley, dando origen a la creación del Instituto Venezolano de los Seguros Sociales, organismo con responsabilidad jurídica y patrimonio propio. Con la intención de adaptar el Instituto a los cambios que se verificaban en esa época, el 5 de octubre de 1951 se deroga la Ley que creaba el Instituto Central de los Seguros Sociales y se sustituye por el estatuto Orgánico del Seguro Social Obligatorio. Posteriormente, en 1966 se promulga la nueva Ley del Seguro Social totalmente reformada el año siguiente es cuando comienza a ser aplicada efectivamente esta Ley, que fundan los seguros de Enfermedades, Maternidad, Accidentes de Trabajo y Enfermedades Profesionales en el seguro de asistencia médica; se amplían los beneficios además de asistencia médica integral, se establece las prestaciones a largo plazo (pensiones) por conceptos de invalidez, incapacidad parcial, vejez y sobrevivientes, asignaciones por nupcias y funerarias.

Se establece dos regímenes, el parcial que se refiere solo a prestaciones a largo plazo y el general que además de prestaciones a largo plazo, incluye asistencia médica y crea el Fondo de Pensiones y el Seguro Facultativo.
En 1989 se pone en funcionamiento el Seguro de Paro Forzoso, mediante el cual se amplía la cobertura, en lo que respecta a Prestaciones en Dinero, a los trabajadores

y familiares; modificándose posteriormente para ampliar la cobertura e incrementar el porcentaje del beneficio y la cotización.

En la actualidad el Instituto Venezolano de los Seguros Sociales (I.V.S.S.), se encuentra en un proceso de adecuación de su estructura y sistemas a fines de atender las necesidades por la población trabajadora.

Misión

El Instituto Venezolano de los Seguros Sociales es una institución pública, cuya razón de ser es brindar protección de la Seguridad Social a todos los beneficiarios en las contingencias de maternidad, vejez, sobrevivencia, enfermedad, accidentes, incapacidad, invalidez, nupcias, muerte, retiro y cesantía o paro forzoso, de manera oportuna y con calidad de excelencia en el servicio prestado, dentro del marco legal que lo regula.

Visión

El Instituto Venezolano de los Seguros Sociales, bajo la inspiración de la justicia social y de la equidad para toda la población, avanza hacia la conformación de la nueva estructura de la sociedad, garantizando el cumplimiento de los principios y normas de la Seguridad Social a todos los habitantes del país. El compromiso social

y el sentido de identificación con la labor que se realiza, debe ser la premisa fundamental en todos los servicios prestados.

Valores

Mantener un ambiente de armonía, colaboración y de gran calidad humana, incrementando así el espíritu de servicio, lealtad y solidaridad en el Instituto, impulsando los siguientes valores:

- RESPONSABILIDAD en nuestras acciones y trabajos encomendados para alcanzar los objetivos propuestos. Reflexionar y valorar las consecuencias de los actos.

- RESPETO a nuestros compañeros de trabajo. Consideración y tolerancia a las diferencias entre los actores internos y externos de la organización.

- EXCELENCIA para ser los mejores en todos los aspectos, con una disposición permanente hacia la mejora.

- LEALTAD con la Institución.

- DISCIPLINA para ser más eficientes en las actividades asignadas.

- ÉTICA profesional en el servicio prestado a nuestra Institución.

- INTEGRIDAD en nuestro trabajo. Actuar con rectitud, honestidad, honradez y transparencia.

Políticas

Enmarcados en lo establecido en el Plan de Patria, SEGUNDO PLAN SOCIALISTA DE DESARROLLO ECONÓMICO Y SOCIAL DE LA NACIÓN, 2013-2019, en su Objetivo General 2.1.1.2. Asegurar la garantía de prestaciones básicas universales relativas a las contingencias de vejez, sobrevivencia, personas con discapacidad, cesantía y desempleo, derivadas de la vinculación con el mercado de trabajo, el Instituto se plantea las siguientes políticas:

- Optimizar los procesos de afiliación y recaudación de cotizaciones que permitan atender a los empleadores o empleadoras, trabajadores o trabajadoras que cumplan con los requisitos de Ley, para disminuir la exclusión al Sistema de Seguridad Social.

- Modernizar los procesos para el otorgamiento de las prestaciones dinerarias, para que las mismas sean otorgadas de forma oportuna y permitan cubrir las necesidades básicas del ciudadano y así, obtener una mejor calidad de vida.

Igualmente, continuando con las líneas del Plan de Patria, en su Objetivo General 2.2.10.1. Asegurar la salud de la población, a través del fortalecimiento continuo y la consolidación de todos los niveles de atención y servicios del Sistema Público Nacional de Salud, priorizando el nivel de atención primaria para la promoción de estilos y condiciones de vida saludables en toda la población; se plantea:

- Promover la atención médica integral a toda la población a fin de garantizar el derecho a la salud y contribuir a mejorar la calidad de vida, el bienestar y la protección a la colectividad.

Estrategias

- Impulsar la simplificación de trámites administrativos y el uso de tecnologías de información para la afiliación de Trabajadores, Trabajadoras, Empleadores y Empleadoras; así como verificar el cumplimiento de los deberes formales y materiales con el Seguro Social.

- Fomentar el desarrollo de herramientas que optimicen el otorgamiento de las prestaciones dinerarias y la continuidad de la protección como derecho adquirido por los beneficiarios.

- Implementar y desarrollar programas de Asistencia Médica Integral, que incluyan los tres niveles de atención.

- Optimizar los procesos para el suministro oportuno de los medicamentos de alto costo a los pacientes con enfermedades crónicas; así como para la aplicación de los tratamientos médicos especializados.

- Adecuar las infraestructuras de acuerdo a la capacidad operativa que deben tener las dependencias, para prestar una atención eficiente a la población demandante de la seguridad social.

- Fortalecer los programas de mantenimiento preventivo y correctivo de las infraestructuras físicas así como de la maquinaria y equipos pertenecientes a las Unidades que conforman el IVSS a nivel nacional.

Bases Éticas y Legales

La constitución de la República Bolívariana de Venezuela contiene en su título IV relativo al Poder Público, cuyas normas se aplican a todos los órganos que ejercen el Poder Público tal como se establece en su articulado, para todos los niveles de la Administración Pública.

Igualmente, para desarrollar todos los principios constitucionales relativos a la Administración Pública, se ha dictado la Ley Orgánica de la Administración Pública.

Como se ha descrito en párrafos anteriores, los procesos de Tecnologías de la Información pueden acarrear delitos informáticos, razón por la cual se deben amparar en la Ley Especial contra Delitos Informáticos.

En resumen las bases legales consultadas en el presente trabajo de grado son las siguientes:

- Constitución de la República Bolívariana de Venezuela, Gaceta Oficial N° 5453 de fecha 24-03-2000. Art. 10.

- Ley Orgánica de Contraloría General de la República y del Sistema Nacional de Control Fiscal, Gaceta Oficial N° 37.347 de fecha 17-12-2001 Art. 82, 83, 84, 85, 91, 93.

- Decreto N° 1.290 del 30-08-2001, con rango y fuerza de Ley Orgánica de Ciencia, Tecnología e Innovación (incluye exposición de motivos) 37291 26-09-2001

- Ley Especial Contra Los Delitos Informáticos, según Gaceta Oficial N° 37313 de fecha 30-10-2001 Artículos:1, 6 al 9 y 15.

- Decreto con rango y fuerza de Ley de Mensajes de Datos y Firmas Electrónicas, Gaceta Oficial N° 37.148 de fecha 28-02-2001.

Bases Conceptuales

En este apartado del documento, se da la definición de los elementos considerados como fundamentales, ya que forman parte de la estructura teórica del tema de estudio.

Administración Pública Nacional: Es un término de límites imprecisos que define al conjunto de organizaciones estatales que realizan la función administrativa del estado.

Modelo: Es la representación abstracta, visual, conceptual de fenómenos, sistemas o procesos, con el fin de detallar o explicar dichos fenómenos, sistemas o procesos. El modelo permite determinar un resultado a partir de unos datos de entrada.

Modelo de madurez: Es un conjunto estructurado de elementos que describen el nivel de madurez de un determinado ente en un aspecto determinado, así mismo, establece de manera explícita la evolución de la organización en dicho aspecto.

Seguridad de la información: Es el conjunto de medidas preventivas y/o reactivas que se toman con la finalidad de garantizar la seguridad de un conjunto de activos de una determinada organización. La información puede encontrarse en distintos medios o formas, no necesariamente en medios informáticos.

CAPÍTULO III

Marco Metodológico

Este capítulo tiene como finalidad describir las fases de la Metodología aplicada, con la finalidad de alcanzar los objetivos planteados en el presente trabajo de investigación. El Marco Metodológico comprende: la población y muestra tomadas en consideración, el instrumento utilizado, el procedimiento realizado para llevar a cabo la investigación y la estrategia empleada para el análisis de los datos obtenidos.

Tipo y Diseño de la Investigación

Una vez que se ha realizado el proceso de indagar en la literatura relacionada con la presente investigación, se han desarrollado las bases teóricas y profundizado con el presente trabajo de tesis en si, se llega a la determinación del tipo y diseño de investigación a ejecutar, para posteriormente definir las estrategias a seguir, enmarcados en este documento, una vez que se ha investigado aquí podemos llegar a la conclusión de que es un proyecto factible apoyado en una investigación documental y de campo.

En el marco de lo conceptual, se tiene que Arias (1999) indica, “La investigación científica es un proceso metódico y sistemático dirigido a la solución de problemas o preguntas científicas, mediante la producción de

nuevos conocimientos, los cuales constituyen la solución o respuestas a tales interrogantes" (p22).

Igualmente Arias (1999, p. 23) establece en torno al Marco Metodológico "La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo la investigación, es el cómo se realizará el estudio para responder al problema planteado".

En un trabajo de investigación realizado por Ana Loly Hernández de la Universidad Pedagógica Experimental Libertador (2010), nos ofrece la siguiente argumentación acerca del proyecto factible "Dentro de la investigación Educativa los Proyectos Factibles se definen como la investigación, elaboración y desarrollo de un modelo operativo viable, cuyo propósito es la búsqueda de soluciones de problemas y satisfacción de necesidades".

El proyecto factible, según documento emanado de la Universidad Pedagógica Experimental Libertador (UPEL) (2003): "Consiste en la elaboración y desarrollo de una propuesta de modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El proyecto debe tener un apoyo en una investigación de tipo documental, de campo o un diseño que incluya ambas modalidades".

El diseño de la investigación según Arias (1999, p. 27) es: “La estrategia que adopta el investigador para responder al problema planteado”

Con respecto a la investigación de campo Arias (1999, p. 33) ofrece el siguiente concepto: “Consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna”.

Definiendo la investigación documental Arias (1999, p. 34) dice: “Es aquella que se basa en la obtención de datos provenientes de materiales impresos u otros tipos de documento”.

Si bien los elementos de la Seguridad de la Información se han ido consolidando a medida que las amenazas existentes en los sistemas publicados en diferentes redes se concretaron y de este modo se puso en evidencia la necesidad imperiosa de contar con elementos que procuren la seguridad de la información que se maneja cotidianamente en la organización.

Se consigue en la actualidad, literatura relacionada con el tema a desarrollar en el presente trabajo de tesis de grado. La teoría de la Seguridad de la Información se ha ido desarrollando y consolidando a medida que el alcance de aplicaciones de redes sociales ha masificado a niveles nunca antes alcanzados, el hecho de compartir información en la Internet.

Ahondando aún más en los tipos de investigación, se encuentra que el diseño de campo se puede dividir según el nivel de profundidad con que se abordan, por lo que puede ser exploratoria, descriptiva, explicativa y evaluativa, se hace mención a estas por ser las más difundidas por los autores en diversos libros de Metodología de la Investigación.

Según Hernandez Sampieri (2008, p. 158), , “El diseño construiría el plan o la estrategia para confirmar los elementos que confirman la o las hipótesis planteadas (...) Si el diseño está concebido cuidadosamente, el producto final del estudio (sus resultados) tendrá mayores posibilidades de éxito para generar conocimiento.

El proceso de recolección de la información necesaria para el desarrollo del trabajo de investigación se prevé que sea de ocho (8) meses, aun cuando los cambios en el área objeto del proceso de indagación, se dan de un modo no expedito comparativamente hablando con respecto al tiempo estimado de recolección de los datos.

Igualmente, se puede ubicar la investigación en un nivel proyectista, definida por Hurtado (2008, p. 72), dado que: “intenta proponer soluciones a una situación determinada a partir de un proceso de investigación. Implica proponer alternativas de cambio, mas no necesariamente ejecutar la propuesta”.

Fases de la investigación

La investigación es un proceso (generalmente cíclico) que combina la teoría con la práctica. La descripción más frecuente del Método Investigación Acción se detalla en un proceso cíclico iterativo de cinco fases. Baskerville (1999, p. 102) identifica cinco fases que interactúan entre si, esto lo podemos visualizar mejor en la siguiente tabla:

Tabla 3: Fases del método investigación acción

Fase	Acción
Diagnosticar	Corresponde a la identificación de los principales problemas que afectan a la organización y que motivan su deseo de cambiar. Envuelve todo lo referente a la interpretación del problema complejo de la organización.
Planificar la acción	Esta actividad específica las acciones organizacionales que deberían tomarse para relevar o mejorar los problemas detectados a diagnosticar. El descubrimiento de los planes de acción es guiado por el marco teórico, el cual indica el estado futuro deseado por la organización y los cambios requeridos para alcanzar dicho estado. El plan establece el objetivo de cambio y el enfoque para cambiar.
Tomar la acción	Implementa el plan de acción. Los investigadores y participantes colaboran en la intervención activa dentro de la organización cliente, provocando ciertos cambios. Diversas estrategias de intervención pueden ser adoptadas: directiva (los investigadores dirigen el cambio), no directiva y tácita.
Evaluar	Una vez completadas las acciones, los investigadores y demás participantes evalúan las salidas. La evaluación incluye determinar si los efectos relevaron a los problemas. Si los cambios fueron exitosos, la evaluación se pregunta si los cambios propuestos fueron los únicos causantes de este éxito. Si los cambios no fueron exitosos, es necesario establecer un marco para la próxima iteración del ciclo de investigación acción.
Especificar el aprendizaje	A partir del resultado de la evaluación, los investigadores especifican el conocimiento adquirido.

Fuente: Baskerville (1999)

Las tareas a desarrollar en cada acción de los procesos estarán sujetas a las condiciones que se creen en cada organización, y pueden emplearse

técnicas y procedimientos diversos, como el benchmarking, la reingeniería, la matriz DOFA, entre otros.

Para iniciar cualquiera de los procesos debe existir la información necesaria y gestionarse correctamente. El resultado de la ejecución de los proyectos que se desarrollan en cada proceso para enriquecer el conocimiento organizacional, puede compartirse entre los involucrados en las actividades llevadas a cabo para fortalecer las medidas orientadas a garantizar la correcta lectura del tráfico de redes de la institución que está siendo objeto de la presente investigación y los resultados obtenidos pueden servir de base para compartir experiencias con diversos entes de la Administración Pública Nacional a través de su interacción en común.

En función de lo anteriormente expuesto, en la Tabla N° 4 se hace una propuesta para las fases del método investigación acción, las cuales son explicadas a continuación.

Revisión documental: Etapa de la fase de Diagnóstico, consiste en la revisión del material bibliográfico relacionado con la definición, las características y experiencias previas que hayan resultado en una contribución al mejoramiento de las prácticas de seguridad de la información. El objetivo es definir un marco conceptual que complemente el trabajo de investigación. El resultado de esta actividad será mostrado en el Capítulo II (Marco Teórico).

Levantamiento de información: Segunda etapa de la fase de Diagnosticar, el objetivo principal de esta actividad será conocer el estatus actual de la Seguridad Informática en el Instituto Venezolano de los Seguros Sociales para indagar en posibles falencias y conocer los motivos que originan ese estado actual de dicha área.

Formulación de la metodología de investigación: Etapa de la fase planificar la acción donde se elabora la adaptación del Modelo de Madurez que se piensa obtener. El objetivo es elaborar el marco metodológico que soporta el presente trabajo de investigación. El presente Capítulo es el resultado de esta actividad.

Diseño del modelo: Primera actividad de la fase tomar acción, para la cual se partirá de los resultados de las actividades anteriores, para diseñar el modelo objeto de esta investigación.

Análisis de contexto: Segunda actividad de la fase tomar la acción, donde se determinan las especificaciones y acuerdos necesarios para implementar el modelo propuesto. El objetivo es preparar las herramientas que se van a sugerir y realizar el correspondiente análisis de contexto donde será evaluada la propuesta.

Evaluación del Método: Así comienza la primera actividad de la fase evaluar, consistirá en presentación de los resultados arrojados por la actividad anterior al modelo propuesto.

Análisis de los resultados: segunda actividad de la fase evaluar, que consistirá en estudiar los resultados a partir de los objetivos planteados en el trabajo de investigación.

Conclusiones: actividad única de la fase especificar el aprendizaje, donde se establecerán algunas recomendaciones relativas al modelo propuesto. Se sugieren algunas recomendaciones para futuros refinamientos del modelo propuesto y para investigaciones futuras relacionadas con el tema de la presente investigación.

Tabla 4: Fases del método investigación acción propuesta.

Fases	Actividades	
1	Diagnóstico	Fase de revisión documental, chequeo de la información suministrada por la Dirección General de Informática, levantamiento de información.
2	Planificar la acción	Adaptar el Modelo propuesto al escenario resultante del proceso de levantamiento de información.
3	Tomar la acción	Diseño del Modelo de Madurez a proponer como plan de acción para llevar el estado actual de la Seguridad de la Información al estado propuesto.
4	Evaluar	Evaluación del Método arrojado por las recomendaciones sugeridas del trabajo de investigación y el juicio de

		expertos involucrados.
5	Especificar el aprendizaje	Conclusiones y recomendaciones.

Fuente: Elaboración propia (2016)

Población y Muestra

La población según Mendenhall (2001, p. 131), “Es el conjunto de todas las mediciones de interés para el investigador que concuerdan con determinadas especificaciones”.

En torno al concepto de población Palella y Martins (2006, p. 226) expresan:, “La población de una investigación es el conjunto de unidades de las que se desea obtener la información y sobre las que se va a generar conclusiones. La población puede ser definida como un conjunto finito o infinito de elementos, personas o cosas pertinentes a una investigación y que generalmente suele ser inaccesible”.

En el caso del presente trabajo, está relacionada a entes e instituciones de la Administración Pública Nacional, tomando entrevistas a personal responsable de la Seguridad de la Información en organismos públicos pertenecientes al Comité de Interoperabilidad, dándose de este modo un caso de especial criticidad, motivado al hecho de que la Seguridad de la Información esta de manera intrínseca relacionada con la Soberanía Nacional.

La institución que ejerce un rol ductor en materia de la Seguridad Informática en la Administración Pública Nacional es la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), a través del VenCERT, que es el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolívariana de Venezuela, cuyo principal objetivo como CERT (del ingles *Computer Emergency Response Team*, Equipo de Respuesta antes Emergencias Informáticas) gubernamental es la prevención, detección y gestión de los incidentes telemáticos generados en los sistemas de información de la Administración Pública Nacional y los Entes Públicos a cargo de la gestión de Infraestructuras Críticas de la Nación.

Se conoce como muestra a un subconjunto seleccionado de la población total de estudio.

Para Sabino (2000, p. 122): “Una muestra, en un sentido amplio no es más que una parte del todo que llamamos universo y que sirve para representarlo”.

Y mas específicamente, con respecto al tema nos dice Sabino (2000, p. 122): “Lo que se busca al emplear una muestra es que, observando una porción relativamente reducida de unidades, se obtengan conclusiones semejantes a las que se lograrían si se estudiara el universo total. Cuando una muestra cumple con esta condición, es decir, cuando nos refleja en sus unidades lo que ocurre en el universo, la llamamos muestra representativa”.

Procurando tener un muestra representativa, se trabajará de manera conjunta con el IVSS particularmente y con personal responsable de la Seguridad de la Información en instituciones pertenecientes al Marco de Interoperabilidad, lo que constituye una muestra no probabilística por conveniencia, donde se tiene que el juicio y la intuición del investigador constituyen un reflejo de la población. Para la investigación actual se procedió a seleccionar personal perteneciente a las siguientes Instituciones del estado, responsables de la Seguridad de la Información:

Tabla 5: Personal de las Instituciones del Estado que respondieron los Instrumentos

Institución	Personal Responsable de la Seguridad de la Información que respondió los instrumentos.
Vicepresidencia de la República	1
Ministerio del Poder Popular de Planificación y Finanzas	1
Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres	1
Comisión de Administración de Divisas	1
Compañía Anónima Nacional Teléfonos de Venezuela	1
Oficina Nacional de Contabilidad	1

Pública	
Servicio Administrativo de Identificación, Migración y Extranjería	1
Servicio Nacional Integrado de Administración Aduanera y Tributaria	1
Servicio Nacional de Contrataciones	1
Superintendencia de Servicios de Certificación Electrónica	2
Instituto Venezolanos de los Seguros Sociales	4
Total	15

: Fuente: Elaboración propia (2016)

los criterios de selección son los siguientes:

•Personal responsable por las instituciones de la Gestión de la Seguridad Informática.

•Personal con conocimientos de los procesos de Seguridad Informática, aún cuando no pertenecieran directamente al equipo de gestión del mencionado proceso.

- Personal experto en la gestión y administración de redes.

La información levantada tiene el compromiso de confidencialidad, se acordó con los entes participantes en el proceso investigativo que dicha información tendrá mero carácter de investigación, esta acotación se hace al personal involucrado en la tarea.

Toda vez que se verifique adecuadamente que los requerimientos sean completamente satisfechos. Se procederá a la entrega del instrumento a todos los miembros de la población que cumplen con los criterios de selección.

Con respecto al aspecto de la división de los tipos de muestra, expresa Sabino (2000, p. 123): “Una primera división que suele hacerse entre las muestras consiste en separarlas en muestras probabilísticas y no probabilísticas”.

- Probabilístico o aleatorio: se aplica si es posible conocer la probabilidad de selección de cada unidad o componente de la muestra.
- No probabilístico: se usa cuando no se puede determinar la probabilidad.

La presente investigación utilizará el no probabilístico, junto con el muestreo intencional, que de acuerdo al criterio de Palella y Martins (2006, p. 120), ocurre cuando el investigador establece los criterios para seleccionar las unidades de análisis, las cuales reciben el nombre de tipo.

Definición de las variables

Disponer de un adecuado sistema de variables es importante en el proceso de investigación ya que facilita todo un diseño, desarrollo y posterior análisis estadístico de los resultados.

Una variable es una cualidad susceptible a sufrir cambios. Según Arias (1994): “Un sistema de variables consiste, en una serie de características por estudiar, definidas de manera operacional, es decir, en función a sus indicadores o unidades de medida”.

Según Sabino (2006, p. 79), “Es cualquier característica o cualidad de la realidad que puede asumir diferentes valores, por lo que pueden ser cualitativas o cuantitativas, tomar valores continuos (pueden tomar infinitos valores) o discretos (toma valores enteros)”.

En este mismo orden de ideas, Bavaresco (1999, p. 41), se refiere a las variables cómo: “Las diferentes condiciones, cualidades características o modalidades que asumen los objetos en estudio desde el inicio de la investigación. Constituyen la imagen inicial del concepto dado dentro del marco”.

Para la presente investigación, las variables estudiadas son las siguientes:

Tabla 6: Definición de las variables de la investigación.

Definición nominal	Rel. Obj.	Objetivo variable	Definición Operacional
Administración Pública Nacional	1	Conjunto de instituciones y organizaciones públicas que realizan la función administrativa y gestión del estado.	Administración Pública Nacional
Instituciones de la APN.	1,3	Identificar las instituciones pertenecientes a la Administración Pública Nacional.	Instituciones de la APN.
Herramientas de Monitoreo Proactivo de Seguridad Informática	3,4	Identificar las herramientas utilizadas para gestionar el monitoreo proactivo de Seguridad de la Información.	Herramientas de Monitoreo Proactivo de Seguridad Informática.
Compromisos legales	1	Asegurar el cumplimiento del marco legal regulatorio en materia de Seguridad de la Información, por parte de los organismos de la APN.	Compromisos legales
Procedimientos de Monitoreo Proactivo de Seguridad de la Información	1,2,3,4	Analizar los procedimiento empleados para el monitoreo actualmente en uso.	Procedimientos de Monitoreo Proactivo de Seguridad de la Información
Adquisición, desarrollo y mantenimiento de herramientas de software.	3,4	Hacer uso de las tecnologías de información para facilitar el proceso de establecimiento de	Herramientas de Gestión y Monitoreo Proactivo de Seguridad de la Información.

		métricas.	
Sistemas expertos	1,2,3,4	Uso de sistemas expertos que permitan tener interfaces de comunicación con los datos recabados en el levantamiento de la información.	•Monitorizar •Diseño •Planificación •Control •Simulación •Instrucción •Recuperación de información.
Modelo de madurez	1,2,3,4	Genera la herramienta que contenga las recomendaciones a seguir para el cumplimiento de las buenas prácticas en materia de Monitoreo Proactivo de Seguridad de la Información.	Modelo de Madurez

Fuente: Elaboración propia (2016)

Instrumentos de diseño del modelo

Para el correcto desarrollo de un instrumento de recolección de datos se debe tomar en cuenta la técnica a emplear, es decir, el procedimiento o forma particular de obtener datos o información.

Según Palella y Martins (2006, p. 126) las técnicas de recolección de variables “Son las distintas formas o maneras de obtener la información, para el acopio de los datos se utilizan técnicas como la observación, entrevista, encuesta y pruebas entre otras”.

Entre los instrumentos usados para llevar a cabo el presente trabajo está la encuesta, que emplea la entrevista como mecanismo para la obtención de datos, según Sabino (2009, p. 155) : “La entrevista, desde el punto de vista del método, es una forma específica de interacción social que tiene por objeto recolectar datos para una investigación”, en este mismo orden de ideas se plantea lo siguiente en torno a la encuesta: “La encuesta es un diseño que se apoya en la entrevista, pero también en otras técnicas. Lo que vulgarmente se llama entrevista es una técnica que en realidad se denomina entrevista no estructurada y lo que suele llamarse encuesta es igual a lo que denominamos en metodología científica, entrevista estructurada”.

Igualmente en los instrumentos de recolección de información tendremos la entrevista la cual según Palella y Martins (2006), “Es una técnica que permite obtener datos mediante un diálogo que se realiza entre dos personas”.

Ahora bien, las técnicas a emplear para el desarrollo del presente trabajo son los siguientes:

- Entrevista en forma de cuestionario para el objetivo específico N° 1. (Anexo D)

- Encuesta para el objetivo general y objetivo específico N° 1.

- Cuestionario para la búsqueda de resultados en los objetivos específicos 1,2,3,y 4.

En las encuestas y cuestionarios desarrollados para el presente trabajo de investigación se va a emplear el siguiente esquema para su formulación:

- Definición nominal de las variables.

- Relación con los objetivos de la investigación.

- Objetivo de las variables.

- Definición operacional de variable.

- Nivel de medición.

Validez y confiabilidad del cuestionario

La validez está relacionada con el grado en que el instrumento mide la variable que se pretende medir, para determinar este parámetro se pueden tomar diversos tipos de evidencias que estén relacionadas con la pertinencia, adecuación o redacción. Según Hernández y Fernández (2006, p. 122), “La medición es un proceso en el cual se vinculan conceptos abstractos con

empíricos, el cual se realiza mediante un plan explicito por lo que implica organizar, clasificar y en ocasiones cuantificar la información".

Adicionalmente, Hernández (2010, p. 122) dice: "Es el grado en que un instrumento realmente mide la variable que pretende medir, que en verdad haga lo que dice hacer".

Según Hernández (2010, p. 122), "Existe una forma de medir la validez, denominada validez por expertos, el cual se refiere al grado en que un instrumento de recolección de datos mide la variable en cuestión, de acuerdo al juicio o criterio de personas calificadas, con amplios conocimientos y experiencia al respecto".

En este mismo orden de ideas, Palella y Martins (2006, p. 82) agregan al mencionado concepto, "El número de expertos puede variar entre tres, cinco o siete, pero que en todo caso dicho número siempre debe ser impar".

En la presente investigación se verificó la validez mediante el juicio de expertos de la Dirección General de Informática, pertenecientes a las Direcciones de Sistemas de Información, Dirección de Telecomunicaciones y Unidad de Seguridad Informática. Se tiene previsto realizar encuestas a personal de las Direcciones antes mencionadas, cinco (5) en total, involucrados en el proceso de diseño e implementación de medidas de seguridad de la información, para su propagación y difusión en la plataforma tecnológica del IVSS.

A estos expertos se les va a suministrar toda la información relativa al tema de estudio, por lo que tendrán a su disposición copias del instrumento y el respectivo formato para el registro adecuado de su juicio en torno a la validez del instrumento, sugerencias y cualquier aporte que pueda recogerse del personal entrevistado.

La finalidad es lograr un instrumento que pueda recoger la información de un modo preciso y se pueda mejorar en sucesivas versiones.

Con respecto a la confiabilidad, Hernández y Fernández (2010, p. 124), “Es el grado en que un instrumento produce resultados coherentes y consistentes, es decir, en caso de ser aplicados consecutivamente sobre la misma muestra y en un espacio corto de tiempo, el resultado debería ser el mismo”.

Para Palella y Martins (2006, p. 83), “La confiabilidad es la ausencia de error aleatorio en el instrumento de recolección de datos, es decir, el grado en que las mediciones están libre de las desviaciones producidas por errores causales.

En la presente investigación para medir la confiabilidad, se utilizará el método de coherencia o consistencia interna, según Hernández y Fernandez (2010, p. 122), “Son coeficientes que estiman la confiabilidad”.

Técnicas para el análisis de los datos

Según Palella y Martins (2006), “Una vez recabada la información, es necesario ordenarla, analizarla para finalmente convertir los datos en conclusiones, los clasifica en datos primarios; los cuales son aquellos que se obtienen directamente de la realidad, sin sufrir ningún tipo de elaboración previa. Los datos secundarios por su parte son aquellos que también han sido tomados de la realidad, pero son sometidos a un proceso, ya sea por el propio investigador o como resultado de estudios previos”.

Una vez que se realice la transcripción de los datos recopilados, se codificaran usando funciones estadísticas de la herramienta de ofimática Calc, para de este modo describir los valores obtenidos en cada una de las variables. Se utilizará la estadística simple para su codificación. Una vez hecho esto, se procederá al graficado y tabulación de los resultados para su muestra.

Procedimiento

El procedimiento utilizado en la realización del presente trabajo de investigación será el siguiente:

- Aplicar el instrumento de medición diseñado.

- Realizar las respectivas mediciones y verificación de la confiabilidad.

- Realizar la codificación, tabulación y graficado de los resultados obtenidos en la aplicación del instrumento.

- Realizar el análisis de los resultados.

- Generar las conclusiones y recomendaciones.

Cronograma de trabajo ejecutado

El cronograma de trabajo tomará un total de 6 meses, contando con la colaboración del personal involucrado en la investigación y generando reuniones quincenales de evaluación y seguimiento.

Tabla 7: Cronograma de trabajo de tesis de grado.

	Duración	**Fecha Inicio**	**Fecha Fin**
Trabajo especial de Grado	200d	02/11/2015	20/05/2016
Levantamiento de información de los instrumentos	15d	02/11/2015	23/11/2015
Revisión bibliográfica y antecedentes.	28d	23/11/2015	20/12/2015
Adaptación de los instrumentos al plano institucional	15d	05/01//2016	19/01/2016
Elaboración de la herramienta para procesar los resultados obtenidos	20d	20/01/2016	08/02/2016
Elaboración de glosario	4d	09/02/2016	12/02/2016
Revisión de la adaptación elaborada con la Dirección General de Informática del Instituto Venezolano de los Seguros Sociales	4d	15/02/2016	18/02/016
Selección de los responsables de cada una de las áreas involucradas	2d	22/02/2016	23/06/2016
Preparación de los instrumentos para ser aplicados en la institución.	4d	24/02/2016	29/02/2016
Implementación de los instrumentos en la institución.	40d	01/03/2016	11/04/2016
Procesamiento de los resultados obtenidos	10d	11/04/2016	22/04/2016
Análisis de los resultados y estudio estadístico de los mismos.	5d	25/04/2016	29/04/2016
Elaboración del informe de los resultados obtenidos	65d	02/03/2016	05/05/2016
Revisiones y ajustes finales a la implementación	5d	09/05/2016	13/05/2016
Presentación de los resultados	1d	19/05/2016	19/05/2016

Fuente: Elaboración propia (2016)

CAPÍTULO IV

Presentación de Resultados

En este capítulo se presentan los resultados obtenidos luego del análisis de los datos, esto como resultado de aplicar el cuestionario elaborado con la finalidad de conocer el nivel de madurez de la institución en estudio.

El mencionado cuestionario fue validado con el juicio de expertos lo que implica que un conjunto de cinco 5 personas reciben el instrumento y el formato para registrar su opinión, adicionalmente se obtuvieron las sugerencias de cada uno de los expertos para la consecución de los resultados esperados, así como de acciones a tomar para las mejoras a aplicar.

En palabras de Cárdenas, F (2005, p. 45), un modelo de seguridad:

Proporciona una representación semántica que describe las propiedades funcionales y estructurales de la seguridad de los sistemas, permitiendo a los desarrolladores trabajar con una definición de alto nivel de los requerimientos de protección y las políticas de seguridad, así como producir una descripción concisa y precisa del comportamiento esperado del sistema.

El autor también expresa que las organizaciones precisan tener altos niveles de seguridad, por esto es que resulta fundamental incorporar un modelo de seguridad con especificaciones formales de los requerimientos y

mecanismos a seguir. Esta aseveración permite hacer una reflexión, y es que también resulta necesario establecer mecanismos que ayuden a mantener los elementos de verificación, para que se mantengan actualizados los elementos de seguridad informática presentes en la red.

En este mismo orden de ideas, Jaurlitza (s.f), expresa que un Modelo de Madurez Tecnológica, "permite valorar el grado de riesgos y vulnerabilidades; asi como marcar la línea a seguir en cuanto a tecnologías, procesos y capacidades de todos los miembros de una entidad determinada, para alcanzar los siguientes niveles de madurez tecnológica".

Sumado a esto, los beneficios que ofrece la aplicación de un modelo de madurez de seguridad de la información según Jaurlitza son:

- Realizar un diagnóstico exacto de la situación tecnológica.

- Proponer el camino de mejora a seguir, para alcanzar el nivel de madurez deseado.

En conclusión, el modelo no es un fin en si mismo, sino una herramienta para conseguir el objetivo compartido por la institución.

En este mismo orden de ideas, Aceituno (2004, p. 123) indica que los modelos de madurez de la Seguridad de la Información (SeI) tienen como objetivo ayudar a las organizaciones a comprender cual es su estado actual

de mantenimiento de la seguridad, y proporcionar una vía para alcanzar el grado de madurez deseado por la organización.

En palabras de Cárdenas, F. (2005, p. 55) los modelos de madurez que se seleccionen para aplicar en una organización deben tener las siguientes características:

- Fácil de comprender
- Implementable
- Carente de ambigüedad
- Capaz de incorporar las políticas en la organización

Por todo lo anteriormente expuesto, la construcción del Modelo de Madurez de Seguridad de la Información de la Información para el Monitoreo y Análisis del Tráfico de redes en la Administración Pública de Venezuela, se puede constituir en un marco de referencia para las instituciones de la APN, en lo relacionado a la Seguridad de la Información. El modelo busca disminuir lo complejo de la gestión de la Seguridad en las instituciones públicas.

Se concluye entonces que se procura comprender el estado actual en que se encuentra la Seguridad de la Información, y contribuir a la formulación de las estrategias que ayuden a las instituciones a alcanzar un nivel de madurez idóneo, con la implementación de las mejores prácticas.

Una vez que se ha avanzado a este punto, se puede afirmar que el modelo busca ser una guía para un acertado diagnóstico y la evaluación de la Seguridad Informática para las Instituciones Públicas, su aplicación y seguimiento buscan minimizar el impacto de potenciales eventos de Seguridad Informática. El modelo considera que la seguridad informática es un proceso y no un problema adicional para la administración de plataformas tecnológicas.

Cabe destacar, que el modelo de madurez integra entre sus niveles las distintas interrogantes que conforman el proceso de seguridad, que según Schneier (2002, p. 93) son:

- ¿Donde queremos estar? (Misión y Objetivos del negocio)
- ¿Donde estamos hoy? (Evaluación)
- ¿Como podemos llegar? (Cambios en el proceso)
- ¿Como saber que llegamos? (Métricas)

Al momento de poner en práctica el modelo de madurez propuesto se van a responder las siguientes interrogantes:

- ¿Que se quiere proteger?
- ¿Contra que se quiere proteger?

- ¿Durante cuanto tiempo se quiere proteger?

- ¿Que presupuesto tiene la Institución destinada para este fin?

Modelo de Madurez de Seguridad de la Información para el Monitoreo y Análisis del Tráfico de Redes en la Administración Pública Nacional.

El modelo se construyó tomando en consideración los aspectos relacionados con la Planificación Estratégica, Cultura Institucional, Dirección, estructura organizacional, los procesos y las tareas; el mencionado modelo esta formado por cinco niveles de madurez y toma como base lo establecido por el Modelo de Madurez de Vicente Aceituno y lo podemos precisar en la siguiente imagen:

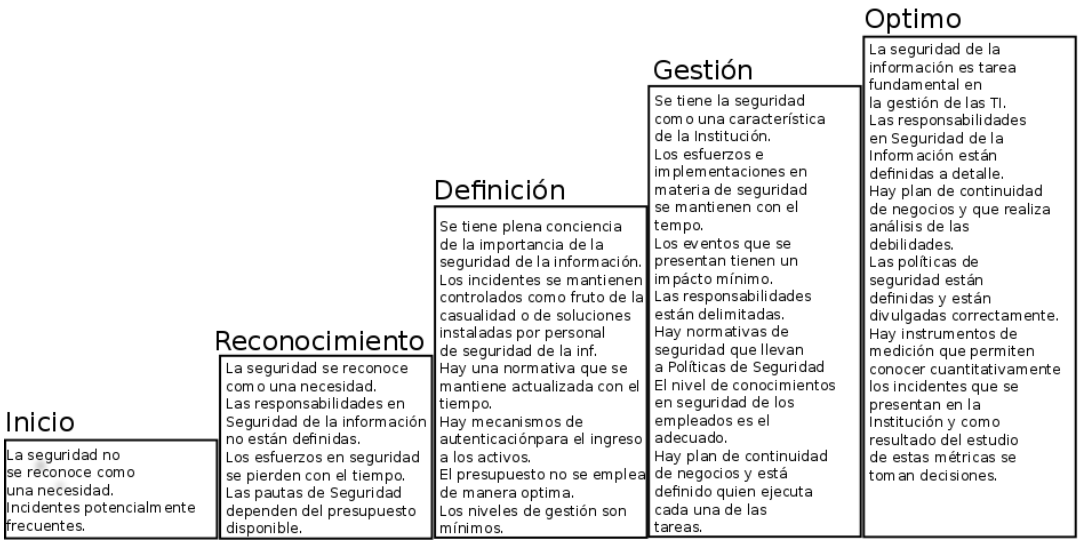

Figura 11: Modelo de Madurez propuesto en la investigación para ser aplicado.

inicio, reconocimiento, definición, gestión y óptimo. Cada nivel posee características que lo definen y en cada uno de los niveles se deben cumplir las características asociadas al mismo y los del nivel que le precede. Cabe acotar que las mencionadas características que forman parte de cada nivel, fueron sometidas al juicio de expertos y adaptadas a las instituciones objeto de la investigación.

Para conocer el nivel en que se encuentran la institución se aplica el cuestionario y con los resultados obtenidos se realiza la correspondiente medición.

Resultados obtenidos de la aplicación del cuestionario

Una vez que se ha aplicado debidamente el cuestionario a las personas involucradas en la investigación se obtuvieron unos resultados que deben ser codificados para poder realizar un análisis de dichos resultados, en el Anexo C, se detallan los resultados obtenidos en cada uno de los ítems asociados a cada pregunta realizada y que permite analizar el estado actual de la Seguridad de la Información en la Institución evaluada. De las respuestas obtenidas se obtuvo una evaluación exploratoria que nos permite determinar los siguientes aspectos, de las áreas en estudio.

Estadísticas asociadas a los incidentes de seguridad de la información

Aunque se tienen evaluaciones periódicas de los incidentes que se originan en la plataforma, no hay en la actualidad un registro detallado de dichos eventos, de manera de poder tomar decisiones fundamentadas en el análisis de los mencionados registros. Por ende, se tiene una gestión reactiva ante la presencia de potenciales incidentes de seguridad informática.

Gestión de las amenazas de seguridad informática

No se tiene una planificación para la recuperación de la plataforma en caso de una eventualidad, la gestión de las amenazas se realiza periódicamente pero igualmente es reactiva y en ocasiones dicha gestión es desbordada por los eventos suscitados.

Identificación y clasificación de activos

Los activos están plenamente identificados, sin embargo no hay una clasificación de los activos, en función del valor de dichos activos, de este modo, si bien se tiene un esquema de protección en función de los activos este esquema es más bien empírico.

Gestión de los riesgos

Se cuenta con medidas para proteger los activos de potenciales ataques internos o externos, sin embargo estas medidas no son puestas a prueba para mediar su efectividad y los eventos en ambiente de producción, son los

que usualmente dan una idea de cuan efectivas son las medidas tomadas con antelación a la ocurrencia de un incidente.

Comité de controles de cambios

Actualmente hay un comité de controles de cambios y dicho comité tiene funciones definidas en el manual de funciones de la Dirección General de Informática, sin embargo, en la práctica el mencionado comité solo tiene carácter informativo, ya que no se reúne periódicamente y no tiene injerencia sobre las decisiones que deben tomarse al momento de realizar cambios sobre la plataforma.

Plan de continuidad del negocio

La institución no cuenta con un Plan de Continuidad del Negocio y de Recuperación de Desastres, al menos formalmente. No se tienen instrucciones precisas de que debe hacer cada uno de los miembros de la Dirección, ante un evento de marca mayor.

Respaldo de la información

Se realizan respaldos periódicos de altos volúmenes de datos, sin embargo no se cuenta con un control efectivo sobre los datos que están siendo respaldados. Los respaldos se almacenan en la misma sede de la Dirección General de Informática, lo que de por si constituye una falla importante en materia de Seguridad de la Información.

Monitoreo de la Plataforma Tecnológica

Se tiene una plataforma de monitoreo de los elementos del área de Infraestructura de Servidores y Telecomunicaciones en la Dirección, sin embargo no se tiene un monitoreo de elementos que se pueden considerar como fundamentales, tales como, métricas del Centro de Datos (Aire, humedad, aterramiento, etc.) Se tienen valores suministrados por las empresas que realizan el mantenimiento en cada una de las áreas pero no hay una medición automatizada y por ende mas fiable de dichos valores.

Monitoreo de la Seguridad de la Información

En la actualidad se tiene software de monitoreo y detección de la seguridad de la información, sin embargo el mencionado software no tiene la parametrización necesaria para poder determinar que valores son los adecuados en materia de tráfico de la red. Igualmente la gestión del tráfico, tal como se plantea en el presente trabajo de investigación, no se realiza con un registro de los valores y evaluación y análisis para la toma de decisiones en esta materia.

Los programas de gestión del monitoreo de seguridad no están centralizados, por lo que eventualmente hay dos visiones de un mismo evento.

Seguimiento y control de los eventos

No hay un programa que centralice los eventos asociados a la Plataforma Tecnológica, hay programas aislados en áreas contiguas, por lo que no se tiene un estudio estadístico preciso y centralizado de los eventos que se presentan y por ende la Dirección no cuenta con herramientas que le permitan conocer cuales son las áreas mas vulnerables, tanto a nivel de software como de hardware.

Nivel de Madurez

El Modelo a emplear en la Institución se construyo a partir de los resultados obtenidos en la implementación de los mecanismos de consulta a los expertos en cada una de las áreas, y de su aplicación a cada una de las áreas involucradas.

Es importante acotar que el Modelo de Madurez sugerido como Aceituno fue adaptado para realizar el trabajo de investigación de acuerdo a las características que presentan las instituciones objeto de estudio en el presente trabajo de investigación.

A saber los cinco niveles a alcanzar son, tal como se mencionó en párrafos anteriores, los siguientes: inicio, reconocimiento, definición, gestión y óptimo, cabe destacar que no siempre es deseable alcanzar el máximo nivel en todos los ítems y cada nivel se alcanza una vez que se ha logrado el nivel anterior.

A continuación se hace una descripción de cada uno de las etapas del Modelos de Madurez,

Inicio

En este nivel la seguridad informática no se reconoce como una necesidad de la institución, se tienen conocimientos adquiridos por individualidades en la institución y los incidentes en seguridad son potencialmente frecuentes y cuando no ocurren se debe a esfuerzos aislados.

Reconocimiento

La seguridad ya es reconocida como característica deseable en la institución. Las responsabilidades de la seguridad de la información no están definidas. Igualmente se dan mas esfuerzos individuales en materia de Seguridad de la Información y los incidentes no ocurren fruto mas de la casualidad que por toma de previsiones. Los esfuerzos suelen desvanecerse con el tiempo, ya que no hay una política de mantenimiento y actualización de la Plataforma Tecnológica.

De manera eventual se realizan evaluaciones de los activos y se efectúan análisis del impacto de un incidente sobre dichos activos.

El presupuesto en materia de Seguridad Informática suele dictar la pauta en cuan elaboradas son las medidas en seguridad de la información.

Definición

En este nivel se tiene plena conciencia de la importancia de la Seguridad de la Información como una necesidad y característica deseable de la institución. Los incidentes de Seguridad se mantienen controlados como fruto o bien de la casualidad, o de soluciones implementadas y mantenidas con el paso del tiempo por personal cuya responsabilidad es mantener una Plataforma de Seguridad.

Hay una normativa que usualmente se mantiene actualizada con el tiempo, se establecen mecanismos de autenticación para el ingreso a los activos de la institución.

Los niveles de gestión no son los deseables, esto como resultado de la ausencia de mecanismos que permitan medir las expectativas, los incidentes y activos de manera constante. Esta medición se realiza de manera esporádica.

El presupuesto de Seguridad de la Información no se emplea de manera óptima, las soluciones de seguridad no suelen ser las más adecuadas para cada escenario.

Gestión

Se tiene la Seguridad de la Información como una característica deseable dentro de la organización, los esfuerzos por evitar los incidentes de

Seguridad Informática son sostenidos en el tiempo y contribuyen a minimizar el impacto de los eventos de Seguridad Informática.

Los eventos que se presentan tienen un impacto mínimo en la plataforma, las responsabilidades en materia de seguridad para atacar dichos eventos están plenamente definidas, lo que garantiza que cada uno de los responsables actúe de acuerdo a lo planificado.

Hay normativas de seguridad que usualmente se llevan a Políticas de Seguridad de la Información, esto permite que el nivel de conocimiento en seguridad de los empleados de la institución sea el adecuado, todo con una correcta divulgación de las mencionadas políticas.

Existe un Plan de Continuidad de Operaciones, que tiene consideración del estado de la Institución y tiene definidos muy a detalle las actividades a desarrollar por cada uno de los responsables de la seguridad.

Las Políticas de Seguridad siempre son aplicadas, se analizan constantemente las expectativas, los incidentes y los activos y en consecuencia se toman las medidas tendientes a mitigar las vulnerabilidades o el impacto provocado por una eventual incidencia.

Óptimo

La seguridad esta reconocida como una característica deseable de la institución, la no presencia de incidentes es un resultado de los esfuerzos

constantes de la institución por evitarlos, todo como consecuencia del análisis de las expectativas, incidentes y activos de la institución.

Las responsabilidades en materia de la Seguridad de la Información están plenamente definidas, esto permite actuar de manera cohesionada ante eventos de seguridad independientemente de la magnitud de dichos eventos.

Se cuenta con un Plan de Continuidad de Operaciones, que considera la evolución constante de la institución a realiza análisis de las debilidades para la posterior toma de decisiones.

Las Políticas de Seguridad están correctamente definidas, son divulgadas y se mantienen actualizadas, adicionalmente se aplican siempre y en todos los casos.

Hay instrumentos de medición que permiten conocer cuantitativamente los incidentes que ocurren en la institución y como resultado de estudios realizados con esta información se toman las decisiones correctas.

Adicionalmente en este nivel de madurez, Aceituno (2006, p. 123) nos complementa los siguientes ítems que además de caracterizar el Nivel Óptimo de madurez nos permite conocer cuales son las condiciones idóneas de seguridad en una organización:

- Se evalúan las expectativas, incidentes y activos cuantitativamente.

• Se toman las mejores medidas disponibles con el presupuesto de seguridad. Se puede determinar si el presupuesto de seguridad es consistente con las expectativas de la organización.

• Las responsabilidades de seguridad en la organización están definidas.

• Existe normativa de seguridad y se aplica.

• Se accede a activos sólo mediante sesiones.

• Se hacen auditorías de las medidas de seguridad.

• Existe normativa de seguridad.

• Hay partición de responsabilidades y son supervisadas.

• Existe un Plan de Continuidad de Operaciones efectivo, que considera la evolución de la organización.

• Se recoge información cuantitativa sobre incidentes y cuasi-incidentes.

• Se seleccionan medidas de seguridad con criterios objetivos.

Resultados del Modelo de Madurez

En el Anexo D se tienen los resultados, con guarismos, del cuestionario aplicado para conocer el estado de la Seguridad Informática en la actualidad.

El cuestionario fue diseñado con diversas alternativas de respuesta, la validación se realizó a través de la técnica del juicio de expertos, lo que implica que dichos especialistas evaluaron el instrumento, dicho cuestionario tenía las siguientes opciones de respuesta: Siempre, Casi siempre, Algunas veces, Casi nunca, Nunca y adicionalmente, tal como se comentó con anterioridad se recibieron las sugerencias y recomendaciones para mejorar el instrumento aplicado.

Escalas para medir las actitudes

Según Hernández (2008, p. 340): “Una actitud es una predisposición aprendida para responder coherentemente de una manera favorable o desfavorable ante un objeto, ser vivo, actividad, concepto, persona o sus simbólicos”. Esto implica que todos los seres humanos tienen una actitud definida hacia diversos objetos, símbolos, etc.

En este mismo orden de ideas, la actitud que tenemos hacia una determinada situación e evento determinará mi manera de actuar ante ese evento en la vida cotidiana.

Hay diversos métodos para medir mediante escalas las variables que se pueden asociar a ciertas actitudes, uno de ellos es la utilización de escalas, entre las más empleadas está la de Likert.

Escalamiento tipo Likert

Roberto Hernández Sampieri (2008, p.341), comenta al respecto de este tipo de escalas: “Este método fue desarrollado por Rensis Likert en 1932, sin embargo, se trata de un enfoque vigente y bastante popularizado. Consiste en un conjunto de ítems presentados en forma de juicios, ante los cuales se pide la reacción de los participantes”.

El mismo autor recomiendo que las frases o juicios deben expresar una relación lógica y que no deben exceder de 20 palabras.

Forma de obtener las puntuaciones.

Según Hernández (2008, p. 346), las puntuaciones se obtienen sumando los valores alcanzados respecto a cada frase. Por ello se denomina escala aditiva. Una puntuación se considera alta o baja según el número de afirmaciones. En la escala de Likert a veces se califica el promedio resultante en la escala mediante la fórmula PT/NT (donde PT es la puntuación total de la escala y NT el número de afirmaciones), donde la puntuación se analiza en el continuo 1-5.

En el presente trabajo de investigación se empleó la escala de Likert donde el promedio resultante tuvo como base la siguiente escala.

Tabla 8: Escala de Likert

1	2	3	4	5
Inicio	Reconocimiento	Definición	Gestión	Óptimo

Fuente: Elaboración: Propia (2016)

Codificación de las respuestas.

Según Hernández (2010, p.348), “Una vez recolectados los datos, estos deben codificarse. Para ello es necesario transformar las respuestas en símbolos o en valores numéricos”. Los datos deben ser preparados para su análisis, porque de lo contrario solo se contaría con número de respuestas.

A cada prioridad se le asignó un valor como se indica en el siguiente cuadro:

Tabla 9: Valorización opciones Modelo de Madurez

Selección	Valor
1	20
2	40
3	60
4	80
5	100

Fuente: Elaboración propia (2016)

Tomando como base este cuadro y los resultados que se tabularon y se muestran en el Anexo C se grafícan los valores y el resultado se puede ver en la siguiente gráfica. Es importante acotar que este procedimiento forma parte de lo propuesto al comenzar el trabajo de investigación, esto es, tener bases científicas para realizar el análisis de los resultados y de este modo sustentar adecuadamente la propuesta generada.

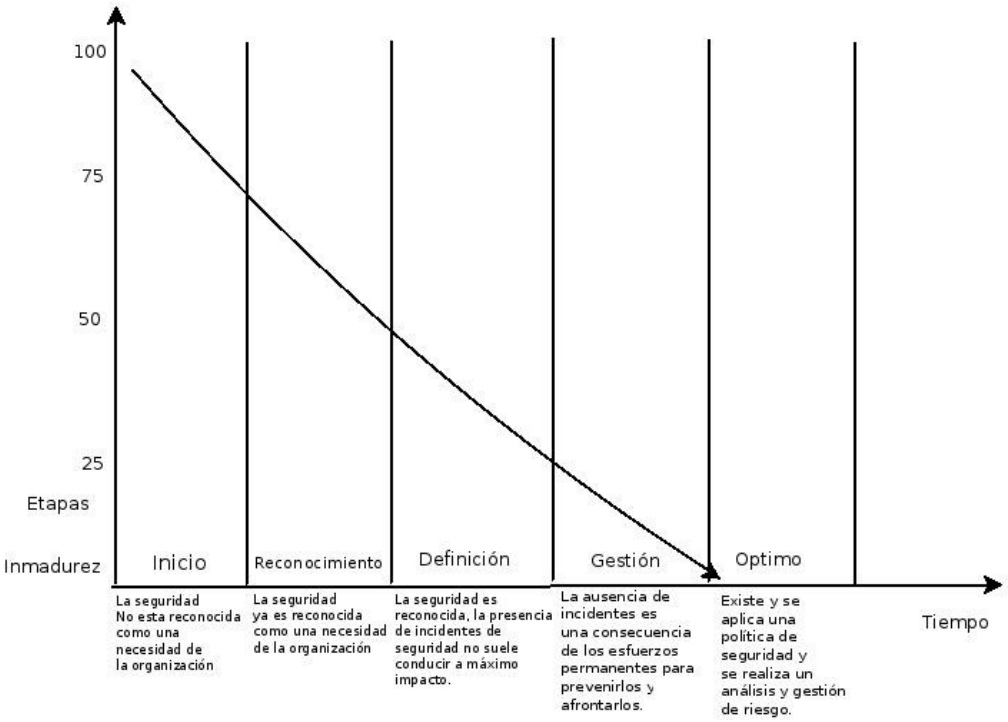

Figura 12: Resultados de la Aplicación del Modelo de Madurez Fuente: Elaboración propia

Luego de realizar los cuestionarios y analizar las respuestas dadas por cada uno de los responsables de las áreas evaluadas se tiene que se debe situar la institución objeto de estudio en el Nivel de Madurez de Definición, donde, si bien se toman las medidas, se realizan los esfuerzos y se planifican compras para cubrir carencias en materia de Seguridad de la Información. la gestión de la seguridad en general tiene características propias del mencionado Nivel de Madurez.

CAPÍTULO V

Conclusiones y Recomendaciones

Esta investigación propone un Modelos de Madurez orientado a realizar mejoras en la gestión de la Seguridad de la Información en la Institución objeto del estudio,

El marco de trabajo propuesto ofrece un conjunto de trabajos a realizar para cumplir los objetivos que se proponen para mejorar la seguridad en la Plataforma Tecnológica.

Los objetivos planteados al momento de emprender la realización del trabajo de investigación fueron cumplidos completamente.

Conclusiones

Luego de realizada la investigación se puede llegar a la conclusión de que aun cuando a nivel tecnológico hay soluciones implementadas para procurar minimizar las vulnerabilidades presentes en la plataforma, la gestión de la seguridad informática tiene serias debilidades.

Las tareas cotidianas en materia de seguridad informática están automatizadas, pero no hay un registro estadístico de los eventos que hayan podido presentarse, de igual manera no hay una documentación actualizada que permita conocer detalles del funcionamiento de la plataforma ante un eventual desastre que precise de dichos registros.

En lineas generales los procedimientos del área de Seguridad Informática tienen poca documentación, las Políticas de Seguridad Informática existen pero no han sido debidamente divulgadas para el personal de la institución.

Los procesos del área de Seguridad Informática y del área Informática en su conjunto son ejecutados por el personal de cada una de las áreas involucradas sin contar con manuales de procesos y procedimientos que les digan que hacer ante cada eventualidad, dicha documentación, tal como se comento previamente en algunos casos existe pero no está actualizada.

El Monitoreo de la Plataforma tal como se describió en lineas previas se realiza, sin embargo el tema de las métricas que permitan ir determinando cuáles son los parámetros adecuados para cada caso se realiza de manera más bien empírica.

No hay un monitoreo de Seguridad Informática propiamente dicho, se tienen herramientas para efectuar esa tarea pero estas no están correctamente parametrizadas y el personal que administra las mencionadas herramientas no cuenta con la formación necesaria para sacar el máximo provecho de estas aplicaciones.

No hay un registro de los eventos o incidentes de Seguridad de la Información, por tanto la toma de decisiones en la materia se ejecutan en función de los reportes que se van generando, de manera que podemos concluir que se tiene una gestión eminentemente reactiva.

La ausencia de políticas bien definidas, ocasiona que no se tenga un marco referencial que pueda servir de apoyo para la toma de decisiones y determine las acciones a seguir en cada eventual caso que pueda presentarse en la cotidianidad.

Se contó con plena participación de los expertos de las diversas áreas que comprenden la Dirección General de Informática de la institución, para completar el cuestionario cuyo objetivo es determinar el nivel de madurez del instituto en cuestión.

Apoyado en el criterio de dichos expertos se determinaron las fases de Modelo de Madurez de la Institución, estas fases son: (0) Inicio, (1) Reconocimiento, (2) Definición, (3) Gestión, (4) Óptimo, se determina entonces que el principal aporte de la investigación es la generación del Modelo de Madurez, aunado a la propuesta de implementación de soluciones orientadas a conformar un marco de referencia en la gestión de la Seguridad Informática Institucional.

Tomando como referencia los resultados obtenidos se determinó que la Institución se encuantra actulamente en el Nivel de Madurez de Definición.

Recomendaciones

Una vez que se tiene una noción del estado actual de la Gestión de la Seguridad Informática y que se tienen identificadas las principales áreas en las que se puede asumir debilidad, se generan una serie de

recomendaciones que pueden coadyuvar a que una vez situados en el nivel de madurez institucional, toda vez que se conozca cuales son los objetivos a alcanzar y cual es el nivel de madurez a donde se quiere llegar, puedan servir para establecer la ruta a seguir y las acciones a tomar.

Es importante acotar que el apoyo al proyecto asociado a la implementación de las soluciones para alcanzar el nivel de madurez deseado, por parte de las máximas autoridades de la institución debe ser el mayor posible. De ser posible el diseño de las acciones a seguir debe contar con la presencia constante de representantes del más alto nivel.

Se debe hacer del conocimiento de todos los involucrados en los procesos institucionales, que el mejoramiento de los procesos de Seguridad Informática deben ser continuos, ya que a la par de que se aplican medidas para incrementar los niveles de seguridad, los potenciales atacantes van diseñando contra medidas para explotar las eventuales vulnerabilidades presentes en nuestros sistemas.

Para alcanzar el siguiente nivel de madurez se recomienda fijar los objetivos a alcanzar para que la gestión de la seguridad de la información se optimice.

Los objetivos a alcanzar pueden ser enumerados de la siguiente manera:

•La Unidad de Seguridad Informática debería reportar directamente a las máximas autoridades de la Institución, en la actualidad esta Unidad forma parte del grupo operativo de la Dirección General.

•Implementar mecanismos que permitan medir el impacto de un incidente de seguridad en la institución.

• Actualización de las normativas de seguridad, aun cuando existen, muchas veces dejan de cumplirse en pos de una rápida respuesta a los requerimientos, sacrificando para esto la seguridad.

•Realización de las auditorías de manera periódica, El trabajo de toma de decisiones debe hacerse en función de los resultados obtenidos.

•Definir las responsabilidades en materia de Seguridad de la Información, de manera precisa.

•Asignar el presupuesto en materia de Seguridad de la Información, y procurar que tengar el uso mas adecuado y las adquisiciones en esta área deben ser acordes con las necesidades reales de la Plataforma Tecnológica.

•La implementación de soluciones de Seguridad de la Información debe ser planificada para que tenga un impacto positivo en la plataforma tecnológica.

•La gestión del Monitoreo de Seguridad de Informática debe incluir herramientas que permitan actuar ante posibles incidentes de Seguridad Informática.

•El monitoreo debe ser proactivo y tomar previsiones ante posibles escenarios que desborden las medidas aplicadas para procurar protección ante eventos de seguridad, esto es la implementación de un plan de recuperación de desastres.

CAPÍTULO VI

Propuesta

A continuación se presenta un marco de trabajo sugerido como resultado del presente trabajo de investigación que debe ser implementado por la Institución para tomar las medidas tendientes a realizar las mejoras y/o correctivos en materia de seguridad de la información.

Esta propuesta, esta basada en los resultados obtenidos y los niveles están orientados a la compatibilidad con estándares tales como:

- ISO27001 (Gestión de la Seguridad de la Información)
- ISO9001 (Sistema de Gestión de la Calidad)
- ISO27001 (Sistema de Gestión de Seguridad de la Información)
- ITIL (Biblioteca de Infraestructura de Tecnologías de la Información)
- CoBIT (Objetivos de Control para la Información y tecnologías relacionadas).

Se determina la necesidad de Implementar una serie de medidas en diversos ámbitos de la Seguridad de la Información, estas medidas serán englobadas en el Plan Integral de Seguridad de la Información (PISI) y se pasa a describir cuáles serían las áreas a estudiar a mediano plazo y qué medidas

se consideran primordiales para procurar alcanzar el Nivel de Madurez adecuado a la realidad de la institución, que situamos en el Nivel de Gestión, de acuerdo al las escalas del Nivel aplicado en el presente estudio.

Objetivos de la Propuesta

El objetivo del presente documento es establecer la metodología de trabajo para la elaboración del Plan de Seguridad Informática de la institución, mediante la descripción de los controles de seguridad que deben ser implementados, de forma que permita la interpretación clara y precisa de las políticas, medidas y procedimientos, que se definan en la misma, con el objetivo de alcanzar niveles de madurez de seguridad que permitan contar con una adecuada gestión de la misma.

Esta metodología está dirigida a delinear adecuadamente las pautas a seguir para la implementación de las medidas que luego de un análisis concienzudo por parte de los especialistas de seguridad informática de la institución se consideran las más adecuadas para lograr parámetros aceptables en materia de prevención de incidentes telemáticos.

Como objetivo principal se tiene alcanzar la implementación de la certificación ISO 27000 en un plazo de dos años, de manera de poder procurar los mas altos niveles de seguridad informática en los diversos aspectos que esta comprende.

Justificación de la propuesta

El Modelo de Madurez para el monitoreo de Seguridad Informática tendrá un impacto altamente positivo para las instituciones del estado, toda vez que la información que manejan los entes estatales son fundamentales para la ciudadanía en general, en cada uno de los casos en que deben interactuar con instituciones para la obtención bien sea de algún beneficio o documentación para su cotidianidad.

La seguridad para los ciudadanos de poder contar con repositorios de datos que son seguros y que van a estar disponibles cuando lo precisen, conlleva una mejora sustancial en la tramitación cotidiana de la ciudadanía.

Marco de trabajo en seguridad de la información

Se han contemplado en todo momento los siguientes puntos para la consecución final de la meta:

Identificar los objetivos de negocio: el propósito de la certificación es garantizar la gestión de la seguridad sin olvidar que esto debe contribuir al desarrollo de los servicios o procesos de negocio. La seguridad debe alinearse estratégicamente con la actividad de la institución para darle un mejor soporte y robustez.

Seleccionar un alcance adecuado: El esfuerzo en la implementación será proporcional al tamaño del sistema a construir. En muchos casos, no es necesario extender el Sistema de Gestión de la Seguridad Informática (SGSI)

a toda la organización sino centrarnos como primer paso en el corazón de la gestión donde se concentra la mayor parte de las actividades relacionadas con la gestión de información, que suele coincidir con las áreas de sistemas de información o con algún departamento donde la seguridad de la información que se gestiona es crítico para el desarrollo de las actividades de negocio.

Determinar el nivel de madurez **:** Debemos identificar en que estado de madurez se encuentra la institución para identificar el esfuerzo que habrá que hacer en la implantación. No va a ser igual en organizaciones que ya han pasado previamente bajo los procesos de certificación de calidad que aquellas que empiecen desde cero y no se encuentren acostumbradas a la gestión de la mejora continua.

Analizar el retorno de inversión: Es muy importante demostrar que el esfuerzo realizado no será un gasto sino una inversión y que tras implantar los procesos de gestión, se conseguirán efectos colaterales que supondrán un retorno de inversión a considerar. Es difícil justificar el ahorro por los incidentes no producidos, pero al menos, si es viable demostrar con indicadores que los índices de incidentes se han reducido.

La planificación de la Seguridad Informática es la expresión gráfica del Sistema de Seguridad Informática diseñado y constituye información básica que establece los principios organizativos y funcionales de la actividad de

Seguridad Informática en la institución y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre la plataforma.

Durante el proceso de diseño del Sistema de Seguridad Informática se pueden identificar claramente tres etapas:

Determinación de las necesidades de protección del o los Sistemas Informáticos que son objeto del análisis, esto incluye lo siguiente:

1.Caracterización del sistema informático.

2.Identificación de las amenazas y estimación de los riesgos.

3.Evaluación del estado actual de la seguridad.

Definición e implementación del Sistema de Seguridad que busca minimizar los rasgos identificados en la primera etapa.

4.Definir las políticas de seguridad

5.Definir las medidas y procedimientos a implementar.

2.Evaluación permanente del sistema de seguridad diseñado.

3.Una vez planteado el problema y las fuentes del basamento teórico, conocer el estado de los fundamentos en Seguridad de la Información, contribuirá con la institución , en aspectos como:

Conocer la aplicación del desarrollo de los dominios de conocimiento más fuertes a nivel de implementación.

•Fortalecer los dominios más débiles.

•Mantener y monitorear los dominios considerados como desarrollados.

•Establecer la consistencia y relación entre los dominios.

•Definir una base para el nivel de la seguridad organizacional, basada en información propia.

•Enunciar algunos basamentos legales que se deben cumplir.

•Establecer lineamientos confiables basados en mejores prácticas.

En los últimos años cuando se ha tratado de ver la seguridad de la información desde un punto de vista general, y se trata de hacer un trabajo preventivo para mitigar estos problemas y vulnerabilidades.

Dominios de Seguridad

Para poder entender este paradigma de trabajo es importante aplicar la teoría de Seguridad de la Información que comprende los siguientes dominios:

- Practicas Gerenciales de seguridad de la información.
- Controles de acceso lógicos a los aplicativos.
- Modelos y arquitecturas de seguridad de la información.
- Seguridad física y lógica.
- Seguridad en redes y telecomunicaciones
- Criptografía.
- Continuidad de negocio.
- Leyes, investigación y ética.
- Seguridad en el desarrollo de aplicaciones y sistemas.
- Seguridad en las operaciones.

Las organizaciones y sus sistemas de información y comunicaciones enfrentan amenazas de un amplio rango de fuentes, incluyendo fraude

asistido por computadoras, espionaje, sabotaje, vandalismo, fuego o inundaciones. Causas de daño como código malicioso, hacking de computadoras y los ataques de denegación de servicios vienen siendo más comunes, más ambiciosos y más sofisticados.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad lograda a través de medios técnicos es limitada, debe ser soportada por la gerencia y procedimientos apropiados. Identificar que controles deben ser usados requiere una planificación cuidadosa y atención en los detalles. Para poder alcanzar Gerencia en Seguridad de la Información y cumplir con todos estos requerimientos es necesario conocer teóricamente como debe gestionarse la Seguridad de la Información en la organización, conocer su estado y empezar a aplicar las mejoras correspondientes.

Levantamiento de información para el total conocimiento de la topología de la red, lo que se constituye en un gran avance con miras a el diseño final ya optimizado, cabe destacar que este diseño estará en constante desarrollo dado que el descubrimiento de nuevas vulnerabilidades siempre estará vigente.

Conformación de un grupo de trabajo que este en avance permanente para la consecución de las metas planteadas, es importante destacar tambien el hecho de que la Unidad de Seguridad Informática debe contar con el apoyo

máximo de la Dirección General y de las autoridades de la Institución para la implementación de las soluciones de Seguridad Informática.

Dentro de las metas mas destacadas que se han alcanzado o que están en fase de consolidación con la planificación efectuada podemos destacar las siguientes:

Analizar los Fundamentos Teóricos en Seguridad de la Información.

• Determinar un ciclo de Seguridad de la Información.

• Conocer e implementar las mejores prácticas en Gerencia de Seguridad de la Información.

• Estudiar las bases de la seguridad en el desarrollo de sistemas y aplicaciones.

• Conocer y establecer los planes de Continuidad de Negocio (BCP) y Recuperación de Desastres (DRP).

• Identificar las leyes venezolanas relacionadas con Seguridad de la Información.

• Establecer la relación entre el estado de los fundamentos teóricos de Seguridad de la Información y certificaciones internacionales como ISO.

Si bien entender el postulado principal de Seguridad de la Información es importante, también lo es comprender el Ciclo de Seguridad de la Información. Se entiende por este al proceso que debe efectuar la organizaciones para cumplir con sus requerimientos de seguridad en las Tecnologías de Información y Comunicación (TIC]), proteger sus activos de información y mitigar los riesgos informáticos.

La alineación de las estrategias de TI con las del negocio son los cimientos de la parte tecnológica, de allí se derivan las estrategias y requerimientos de seguridad de la información. La idea es planificar la seguridad creando políticas, estándares y procedimientos por los cuales se van a regir y gobernar los usuarios de las TIC en la Institución.

Seguidamente se realiza la valoración del riesgo informático, donde se determina su prioridad y el riesgo tolerable por la Institución. Una vez realizada esta valoración se deben realizar las acciones necesarias para aceptar, transferir, ignorar o mitigar el riesgo hasta el nivel acordado.

A partir de la mitigación se procede con el monitoreo y control de todos los procesos dependientes de Seguridad de la Información y se obtienen valores para los indicadores, es allí cuando toma participación los procesos de mejora continua, auditorías internas y externas y la parte legal, para reanudar el ciclo con la periodicidad explicita en las políticas, estándares y procedimientos. También es importante el manejo de los incidentes, ya que

sirve de ayuda para eventos inesperados, vulnerabilidades nuevas o no identificadas que sea necesaria su mitigación en un periodo de tiempo aceptable.

Propuesta de Indicadores de Gestión y Estadísticas para la Unidad de Seguridad Informática

Actualmente la Unidad de Seguridad Informática Informática se encuentra laborando bajo 11 Procesos levantados en la Unidad de Seguridad Informática, los cuales abarcan, entre otros, las principales funciones rutinarias que se llevan a cabo por el personal destinado para ello.

Los procesos definidos actualmente son :

1.Creación, Desactivación y Modificación de usuarios

2.Concesión de Permisologías para el acceso a los servicios de la Red

3.Soporte en la configuración de Antivirus

4.Instalación y Configuración de cuentas Redes Privadas Virtuales, conocidas como VPN

5.Mantenimiento de las Normas y Procedimientos a Nivel de Seguridad Informática

6.Análisis de incidentes de seguridad informática

7.Monitoreo de los Aplicativos, servicios y equipos que conforman la Red

8.Auditoría los sistemas y servicios de la red

9.Ejecución de Controles de Cambio (CDC)

10.Ejecución de Respaldos de los servicios

11.Generación de Estadísticas

A través de éstos procesos se procura plasmar, a través de un lenguaje claro y sencillo, la metodología paso a paso para determinar y mantener informado al personal de la Dirección de Seguridad de la Información (DSI) acerca de cómo ejecutar las actividades correspondientes para cumplir el fin de cada proceso. Cada uno de los procesos antes indicados se encuentran definidos, diagramados y tabulados.

Luego de la necesidad presentada por la Unidad de Seguridad Informática Informática, acerca de la ausencia de mecanismos de medición automatizados, que permitan evaluar, comparar, analizar y tomar acciones relacionadas a las actividades de la DSI, se elaboró un análisis de cada uno de los procesos definidos, evaluando los siguientes parámetros:

- Entradas y salidas de los procedimientos.

- Los procesos son transversales con otras unidades de la institución.

- Correspondencia de los nombres, con las actividades y conceptos de los mismos.

- Estipulación de todas las actividades de la DSI con todos los procesos.

Obteniendo como resultado, el siguiente análisis:

- Ausencia de procesos que son vitales para el mantenimiento de la Plataforma de Seguridad.

- Existencia de procesos manuales que deberían funcionar de manera automatizada.

- Ejecución de Respaldos de los servicios DSI

- Generación de Estadísticas

- Procesos definidos que actualmente no se ejecutan.

- Auditoría a los sistemas y servicios de la red

- Ausencia de plantillas o formatos que determinen el cumplimiento del proceso.

Asimismo, se evaluaron las estadísticas que actualmente son entregadas a la Dirección General de Informática. La fuente de datos fueron diversos correos y documentos de la carpeta compartida, con la siguiente información:

Tabla 10: Fuentes de datos de la Unidad de Seguridad Informática

Estadísticas (EST)
Licencias instaladas por región, fuente: SGDS/BD AV
Adm de usuarios: creación, modificación y desactivación/ fuente: BD RT
Adm acceso a la red: configuración, permisología, seguimiento y soporte/ fuente BD RT
Requerimiento por región, fuente: BD RT

Fuente: Elaboración propia (2016)

De éstos datos, se generaron las siguientes conclusiones:

1.La clasificación del campo Administración de acceso a la red, a nivel de análisis, no brinda información relevante para la toma de decisiones y ejecuciones de acciones correctivas.

2.El campo de Requerimiento por Región, debería mostrarse de manera desglosado, debido a que no muestra clasificación por tipo de requerimiento, lo que no permite trabajar con un espectro claro acerca de las necesidades de las regiones.

3.Ausencia de datos que permitan tomar acciones correctivas relacionadas a la seguridad de la plataforma del IVSS.

4.Los datos no se obtienen de manera automatizada.

5.Las estadísticas deberían alimentarse de los resultados de la ejecución de los procesos junto con sus respectivos indicadores.

Además se llevo a cabo un estudio de las aplicaciones utilizadas por la DSI, a fin de indagar la fuente de los datos que son extraídos para estadísticas y demás informes presentados por la división, determinando lo siguiente:

Tabla 11: Tabla de aplicaciones

APLICACIÓN	RT Rt-seguridad.ivss.int	Sistema de Gestión de la División de Seguridad segapp.ivss.int:8080/seguridad	monitoreo.ivss.int		colector.ivss.int	Colector: OCS inventory	nacional.antivirus.ivss.int	Intranet w3.ivss.gob.ve
			Nagios	Cacti				
DATOS	Configuración /Fuente BD (EST)	Ciudadanos y plantilla de trabajadores del IVSS	Estado de los servicios (IVS)	Gráficos (IVS)	Del Colector no se extrae información para estadísticas o informes regulares. La información que colector suministra para informes, es extraída directo del Nagios	Activos de los dispositivos que son responsabilidad de la división de seguridad	Informe total clientes reportados por región, fuente: Informe ERAC **	.
	Permisología /Fuente BD (EST)	Inventario servicios, fuente:	Estado de los routers (IVS)				Amenazas principales / clientes, fuente: informe ERAC **	
	Seguimiento /Fuente BD (EST)	Inventario redes, fuente:	Comportamiento de los enlaces (IVS)				Amenazas principales , fuente: Informe ERAC	
	Soporte /Fuente BD (EST)	Firewall						
	Usuario /Fuente BD (EST)	Casos atendidos por analista, fuente: RT						
	Mantenimiento /Fuente BD (EST)	Casos atendidos por región, fuente: RT						
		Casos atendidos por tipo, fuente: RT						
		Usuarios activos, fuente: LDAP (RANGOS DE FECHA)						
		Usuarios desactivos, fuente LDAP						
		Usuarios no personalizados, fuente: LDAP						
		Usuarios con claves predeterminadas, fuente: LDAP						
		Licencias instaladas 2012 por región: base de datos AV (EST)						
		Licencias reportadas 2012 por región: informe ERAC **						
		Amenazas latentes: base de datos AV						
		Amenazas por región: base de datos AV						
		Proxy de navegación DGI y Altagracia, fuente:						
		Navegación de Usuarios por Proxy, fuente:						
		Clientes reportados, fuente: Informe ERAC						
		Amenazas principales / clientes, fuente: informe ERAC **						
		Antispam, fuente: srvds0601.ivss.gob.ve						

Fuente: Elaboración propia (2016)

De éstos datos levantados, se determinó que existen dos aplicativos mostrando la misma información, ejemplo de ello, Amenazas principales / clientes, información visualizada en la aplicación de DSI y en la aplicación de Antivirus.

Propuesta de indicadores de gestión

A fin de obtener datos precisos, relevantes, automatizados, que permitan alimentar a diversas herramientas de análisis, se propone evaluar la operatividad de la oficina,mediante la aplicación de Indicadores en su variable de Gestión.

Los indicadores de gestión se miden a través de los procesos definidos, permitiendo mejorar la utilización de los recursos físicos, técnicos y humanos en el cumplimiento de metas y objetivos de la Dirección General de Informática, como también ayudar en la toma de decisiones.

Para la elaboración de los siguientes indicadores, se deberán modificar algunos de los Procesos levantados con anterioridad, con el fin de determinar los documentos finales que serán base para la medición de algunos de los indicadores, además de establecer de manera granulada cada una de las actividades que se deberán llevar a cabo para el cumplimiento de la meta de cada uno de los indicadores.

Tabla 12: Tabla de procesos de la Unidad de Seguridad Informática

N	PROCESOS	INDICADOR DE GESTIÓN	¿QUÉ SE MIDE?	FUENTE DE INFORMACIÓN*	¿PARA QUÉ SE MIDE?
1	Creación, Desactivación y Modificación de usuarios **LDAP**	Índice de creaciones de usuarios en el LDAP	Cantidad de creaciones de usuarios en el LDAP	RT	Medir operatividad
		Índice de desactivaciones de usuarios en el LDAP	Cantidad de desactivaciones de usuarios en el LDAP	RT	Medir operatividad
		Índice de modificaciones de usuarios en el LDAP	Cantidad de modificaciones de usuarios en el LDAP	RT	Medir operatividad
2	Concesión o denegación de permisologías para el acceso a los servicios de la Red	Índice permisologías suministradas	Cantidad de permisologías brindadas	RT	Medir operatividad
		Índice de denegaciones	Cantidad de denegaciones	RT	Medir operatividad
3	Mantenimiento de la plataforma de **Antivirus**	Índice configuración antivirus	Cantidad de soportes brindados en relación a la confi	RT	Medir operatividad
4	Concesión o revocación de cuentas **VPN**	Índice cuentas VPN asignadas	Cantidad de cuentas VPN asignadas	RT	Medir operatividad
		Índice cuentas VPN revocadas	Cantidad de cuentas VPN revocadas	RT	Medir operatividad
5	Mantenimiento de las Normas y Procedimientos a Nivel de Seguridad Informática	Índice manuales de normas y procedimientos revisados seg	Cantidad de normas y procedimientos relacionados a	Manuales de Normas y Procedimient	Medir operatividad
		Índice manuales de normas y procedimientos revisados seg	Cantidad de normas y procedimientos relacionados a	RT	Medir operatividad
6	Análisis y atención de incidentes de seguridad informática	Índice de análisis de incidentes detectados en otras unidad	Cantidad de incidentes de seguridad detectados y an	RT	Medir operatividad
		Índice de incidentes DSI resueltos	Cantidad de incidentes de seguridad resueltos	RT	Medir operatividad
7	Monitoreo de los aplicativos, servicios y equipos que conforman la Red	Índice de informes de verificación	Cantidad de monitoreos ejecutados	Nagios/CACTI	Medir operatividad
8	Auditoría a los sistemas y servicios de la red	Índice de auditorías de sistemas y servicios de red	cantidad de auditorías llevadas a cabo según planific	Planificación 2012	Medir operatividad
9	Ejecución de Controles de Cambio (CDC)	Índice de controles de cambio	Cantidad de controles de cambio en los que DSI ha i	RT	Medir operatividad
10	Análisis de Estadísticas	Índice de estadísticas analizadas	Cantidad de estadísticas analizadas	SEGapp	Medir operatividad
11	Mantenimiento de la plataforma de seguridad	Índice de mantenimientos para el Firewall	Cantidad de mantenimientos llevados a cabo en el Fi	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Asa	Cantidad de mantenimientos llevados a cabo en Asa	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Proxy	Cantidad de mantenimientos llevados a cabo en Prox	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Antivirus	Cantidad de mantenimientos llevados a cabo en Anti	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Antispam	Cantidad de mantenimientos llevados a cabo en Anti	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el VPN	Cantidad de mantenimientos llevados a cabo en VPN	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Respaldo	Cantidad de mantenimientos llevados a cabo en Res	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Logs	Cantidad de mantenimientos llevados a cabo en Logs	Planificación 2016	Medir operatividad
		Índice de mantenimientos para el Tacacs	Cantidad de mantenimientos llevados a cabo en Taca	Planificación 2016	Medir operatividad

Fuente: Elaboración propia (2016)

A su vez el resultado de los indicadores de gestión, en algunos casos, alimentarán las estadísticas que deberán ser entregadas a la Dirección General de Informática.

Igualmente, se propone la modificación o programación de un único site para la extracción de datos, a fin de evitar la redundancia de datos.

REFERENCIAS BIBLIOGRÁFICAS

Fuentes Impresas

Aceituno, V. (2007).*Seguridad de la Información*. México. Limusa Noriega

Alexander A. ((2007), *Diseño de un sistema de gestión de seguridad de información*, (1rq ed), Colombia Alfaomega

Álvarez, G., y Pérez, P., (2004). Seguridad Informática para Empresas y Particulares. pp. 8388

Anderser E.S y S.A. Jensen (2006), *Project mantury in organization*, international journal of project management, vol 21, issue 6, august (2006)

Arias F.. (2006), *El proyecto de investigación*, (5ta ed.), Caracas, Venezuela: Episteme.

Ballestrini, M. (2002). *Cómo se Elabora el Proyecto de Investigación*. (6ª Ed.).Caracas. BL Consultores Asociados, Servicio Editorial.

Barrios Y. (2010), *Manual de trabajo de grado de Especialización y Maestría y Tesis Doctorales,* (4ta ed.), Venezuela: FEDUPEL.

Baskerville, R. (1999). Investigating Information Systems with Action Research.Communications of the Association for Information Systems.

Bauer, M (2005), Seguridad en servidores Linux, Madrid: Ediciones Anaya

Bautts, T. (2005), Linux Guía para administradores de redes, Madrid: Ediciones Anaya.

Bavaresco, A. (2006). Proceso Metodológico en la Investigación. (Cómo hacer un diseño de investigación). Maracaibo: La Universidad del Zulia.

Brotby, K. (2009), Information security management metrics. A definitive guide to effective security monitoring and measurement. CRC Press.

Carracedo, J., (2004). Seguridad en Redes Telemáticas. Universidad Politécnica de Madrid. McGraw-Hill/Interamericana de España.

Cheswick, W., y Bellovin, S., (1994). Firewalls and Internet Security: Repelling the WilyHacker. Addison-Wesley professional computing series. Addison-Wesley, Reading, MA-USA.

Chiavenato, I. (2004), *Iniciación a la administración de la producción*, México: Mc Graw Hill.

Estay-Niculcar, C., (2006) Aplicación estratégica de tecnología en la Dirección y Gerencia en el Entorno Latinoamericano. Fundación Universitaria Iberoamericana FUNIBER

Expósito, F.,(2003). Metodología de Análisis y Gestión de Riesgos: MAGERIT. Seguridad en Redes Telemáticas.

Fábregas, J. (2009). Tecnología de Información Gerencia de Servicios Basado en ITIL. Caracas: Universidad Católica Andrés Bello.

Fábregas, J. (2008). Tecnología de Información Planificación, Análisis y Diseño (UML- Estructurado). Caracas: Universidad Católica Andrés Bello.

Ford, M y Spanier S. (1998), Tecnologías de Interconectividad de redes, Mexico: Prentice-Hall.

Gómez, A., (2006). Enciclopedia de la Seguridad Informática. Ra-Ma Editorial. Madrid.

Gordillo Mejía, Abraham (2008), Desarrollo y aprendizaje organizacional: paradigmas del siglo XXI, Editorial Trillas, Mexico.

Gottschalk, P. (2003), Gestión del conocimiento en las empresas de servicios profesionales: estudio de la utilidad de la TI en los bufetes de abogados, en Sistemas de gestión del conocimiento. Teoría y práctica, editor Stuart Barnes, Colección Negocios, Thompson Editores, España, pp 97-111.

Hernández R. (2010). *Metodología de la investigación*, Caracas: Editorial Mc Graw Hill.

Hernández, R., Fernández, C., y Baptista, P., (2003) Metodología de la investigación (3a. ed.). México: McGraw-Hill Interamericana.

Hurtado, J. (2008). *Cómo Formular Objetivos de Investigación*. (2 ª Ed.). Caracas. Ediciones Quirón.

Hurtado, J. (2010). *El Proyecto de Investigación, Comprensión holística de la metodología y la investigación*. (6ª Ed.).Caracas. Ediciones Quirón.

Hyden, L. (2010) *IT Security metrics. A practical framework for measuring security & protecting data*. McGraw Hill.

Jaquith, A. (2007) Security metrics. Replacing fear, uncertainty, and doubt. Addison Wesley

Laudon, K., y Laudon, J., (2002). Sistema de Información Gerencial. Pearson Educación. 6Ta edición.

McCarthy, M., y Campbell S., (2002). Seguridad Digital. Estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía. Madrid: McGraw-Hill de Management.

McNab, C. (2008). Seguridad de Redes, Madrid: Ediciones Anaya

Mendenhall, W y Reinmuth, J., (2001). Estadística para administración y economía. IBEROAMERICANA , MEXICO.

Namakforoosh M. (2001). *Metodología de la investigación*, México: Limusa. 1987. ME.

Nolan, R., (1979).Managing the crises in data processing. Harvard Business Review. March.

O'brien J. y Marakas G. (2006). *Sistemas de información gerencial*, (7 ª Ed.). México: McGraw-Hill.

Oppleman, V. (2005), Extreme Exploits, Madrid: Ediciones Anaya

Pacheco, F. y Jara, H (2009). Hackers al descubierto, Buenos Aires: Ediciones Sevagraf.

Palella S. y Martins P. (2006). *Metodología de la investigación cuantitativa*, (2ª ed.), Venezuela: Fedupel.

Parra Manzano, G. (2005). Manual de Derecho Administrativo General. Valencia: Vadell Hermanos C.A.

Pazos J. (2009). Gestión de la información y del conocimiento, Madrid: Centro de Estudios Finanacieros.

Sabino, C. (1999). El *proceso de la investigación*, Caracas: El Cid Editor.

Sampieri, Roberto (2006), "Metodología de la investigación", México.

Schneier, B., (2002). Secrets and Lies. Digital Security in a Networked World. USA: Edition John Wiley & Sons.

Schroder, C (2008). Redes en Linux Guia de referencia, Madrid: Ediciones Anaya.

Seatón y Bresó (2001), “Gerencia del Conocimiento”, Revista Espacios, Vol. 22, Num. 3, Venezuela.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes, Aplicaciones y Estándares*. (2ª Ed.). Madrid. Pearson Education, S.A.

Tamayo y Tamayo, M. (1996). *El proceso de la investigación científica*. (3er. ed.). México: Limusa.

Trabajos y Tesis de Grado

Barrios M. (2004). Aplicación de un Modelo de Madurez de Gerencia de Proyectos para un Institución Bancaria. Universidad Católica Andrés Bello. Caracas.

Begun Ö. (2009). *Riesgo de evaluación de la gestión de vencimiento: Un marco para las empresas de construcción*. Universidad Metropolitana, Caracas.

Hernandez F. (2011). Desarrollo de un Modelo de Madurez para las Contingencias y Recuperación de la Información en las Pequeñas y Medianas Empresas del Sector Salud en Venezuela. Universidad Católica Andrés Bello, Caracas.

Ortiz L. (2012). Modelo de Gestión de Procesos de Servicios de Tecnología de Información Basado en Librerías de Infraestructura de Tecnologías de Información (ITIL) para la Administración Pública Nacional. Universidad Católica Andrés Bello, Caracas.

Valdéz G. (2010). Modelo de Madurez y Capacidad de Implementación de Gobierno Electrónico en Instituciones Públicas. Universidad Técnica Federico Santa María, Valparaíso, Chile.

Villegas M. (2008). Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades. Universidad Simón Bolívar, Caracas.

Referencias Electrónicas en Línea

SUSCERTE (2011). Superintendencia de Servicios de Certificación Electrónica. Recuperado el 22 de Enero de 2016, de www.suscerte.gob.ve

IVSS (2008). Instituto Venezolano de los Seguros Sociales. Recuperado el 10 de Febrero de 2016, de www.ivss.gob.ve

ISACA (2008). IT Gvernance Institute. Recuperado el 10 de Enero de 2016, de http://www.isaca.org/about-isaca/it-governanceinstitute/pages/default.aspx

SEI (2001). Software Engineering Institute. Recuperado el 10 de Enero de 2016, de www.sei.cmu.edu

Ostiasis. (2011). Ostiasis. Recuperado el 30 de Enero de 2016, de Especialistas en

Gestión de Infraestructura de TI: www.osiasis.es

RAE (2005). Real Academia Española. Recuperado el 15 de Enero de 2016, de www.rae.es

ANSSI (2002) Agence Nationale de la Securite des systemes d'information. Recuperado el 19 de Enero de 2016, de www.ssi.gov.fr

Revista Espacios (2005) Gestión del conocimiento organizacional y en la teoría de las relaciones humanas. Recuperado el 22 de Enero de 2016, de http://www.revistaespacios.com/a05v26n02/05260242.html

Libros en línea.

Best Management Practices, ITIL Version 3, (2007), [Libro en línea], Consultado en Enero 2016 en: www.best-management-practice.com/itil.

COBIT 4.1 (2005) IT Governance Institute, [Libros en línea], impreso en Estados Unidos de América, Consultado en Enero 2016 en: http://www.itgi.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf.

ISO/IEC 17799, Organización Internacional de Estandarización,(2005), Consultado Enero 2016 en: http://sgsi-iso17000.blogspot.com/2007/09/iso-17000-en-castellano.html

ISO 27002, Organización Internacional de Estandarización (2005), Consultado Enero 2016 en: http://sgsi-iso27001.blogspot.com/2007/09/iso-27001-en-castellano.html

Fuentes Electrónicas.

Anamias P. (2004). *Testing de sistemas en tiempo real,* http://itaim.vtrbandaancha.net/paper/Investigacion.pdf, [Consultado: 2016, enero]

Andreus L. (2000), *Reingeniería en los procesos de negocios*, http://prof.usb.ve/lmendoza/Documentos/PS-6116/Teor%EDa %20PS6116%20Reingenier%EDa.pdf, [Consultado: 2016, Enero]

Bunge M. (1989), La ciencia, su método y su filosofía, http://users.dcc.uchile.cl/~cgutierr/cursos/INV/bunge_ciencia.pdf [Consultado: 2016, Febrero]

Cañizares, R. (2010). Arboles de ataque una herramienta imprescindible en la protección de infraestructuras críticas. [en línea]. México. Recuperado el 5 de febrero de 2016, de: http://es.slideshare.net/cprti/rboles-de-ataque-una-herramienta-imprescindible-en-la-proteccin-de-infraestructuras-crticas

Gómez, L., Farías-Elinos, M., Mendoza, M. (2003). Importancia del Análisis de Riesgo d Seguridad.

Disponible:
http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/impariesgo.pdf.
[Consultado: 2008, enero 10]

Hernandez A. (2010). El proyecto factible como modalidad en la investigación educativa, https://luiscastellanos.files.wordpress.com/2014/02/el-proyecto-factible-como-modalidad-en-la-investigacion-educativa-ana-hernandez.pdf

[Consultado: 2016, Enero]

Microsoft (2004). *Guía de Administración de Riesgos de Seguridad* [en línea] http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx.
[Consultado 2016, Enero]

Sancho y Cervera, J., (s.f). Habitat. Secretaria de Desarrollo Social. Modelo de Mejores

Prácticas para el Transporte Público Urbano y otros Servicios Municipales. México. Disponible: http://www.habitat.gob.mx/modelos/guiasmetodologicasytecnicas/libro_mp.pdf. [Consultado: 2016, Febrero 14].

Urbaez, M. (2005). Gestión del conocimiento organizacional en el taylorismo y en la teoría de las relaciones humanas. Disponible: http://www.revistaespacios.com/a05v26n02/05260242.html [Consulta: 2016, enero 31]

ANEXO A

CUESTIONARIO

El objetivo del presente instrumento es conocer el estado actual de la Seguridad Informática en la Plataforma institucional para la que usted trabaja, esto enmarcado dentro de un trabajo de investigación orientado a determinar ese estado en la Administración Pública Nacional de Venezuela.

La investigación procura medir el estado de madurez del Monitoreo de Seguridad Informática para tomar las correspondientes medidas y por ende incrementar los niveles de seguridad en la mencionada plataforma.

Las personas seleccionadas para responder esta encuesta son un grupo de expertos con cuyo criterio se busca tener parámetros que permitan establecer las métricas necesarias con el propósito ya mencionado.

Se precisa que las respuestas dadas al presente cuestionario sean dadas con las mayor objetividad posible, esta dividido en dos partes, una primera que tiene preguntas con respuestas tipo Si o No y una segunda parte donde se pide que de prioridad a una serie de interrogantes relacionadas con el estado de la Seguridad Informática en la Institución.

En ambas partes debe marcar con una X la opción que corresponde a su selección, solo puede marcar una a la vez.

De antemano muchas gracias por su valiosa colaboración en la consecución del éxito de la presente investigación.

Apellidos y Nombres:_____

Institución para la que trabaja:_____

_____

Cargo que desempeña:_____

Departamento: _____

Profesión:_____

Años de experiencia:_____

NIVELES DE MADUREZ DE LA ADMINISTRACIÓN PÚBLICA NACIONAL EN LA GESTIÓN DEL MONITOREO DE LA SEGURIDAD INFORMÁTICA

CARACTERÍSTICAS ORGANIZACIONALES

Instrucciones: Lea cada una de las preguntas y responda de acuerdo al contexto donde labora.

	NIVEL DE INICIO	SI	No	NS/NC
1	¿Existe un departamento encargado de la Seguridad Informática en la Institución?			

	NIVEL DE RECONOCIMIENTO	SI	NO	NS/NC
1	¿Existe una persona encargada de la Seguridad de la Información?			
2	¿Las personas que conforman el departamento encargado de la Seguridad Informática son del área Informática?			
3	¿Las personas que laboran en el departamento de la seguridad tienen experiencia en el área?			
4	¿Hay herramientas de seguridad como antivirus en la plataforma institucional?			
5	¿Hay herramientas de seguridad como detector de intrusos en la plataforma institucional?			
6	¿Hay herramientas de seguridad como proxies en la plataforma institucional?			
7	¿Tiene la plataforma institucional herramientas como firewall de sotfware?			
8	¿Tiene la plataforma institucional herramientas como firewall de hardware?			

9	¿Tiene instalada en la plataforma institucional alguna otra herramienta de software antiespias?			
10	¿Hay un departamento encargado de la seguridad física de la información en la institución?			
11	¿Existen políticas de seguridad que determinen la responsabilidad de la aplicación de medidas de seguridad en la Institución?			
12	¿Tiene la institución instalada herramientas que permitan conocer el estado del tráfico de redes en la institución?			
13	¿Existe un marco de trabajo de la Seguridad de la Información en la institución?			
14	¿Los programas instalados en las aplicaciones son actualizados regularmente?			
15	¿Se realizan copias de respaldo y recuperación de datos en la institución con regularidad y niveles de retención?			

Si considera que falta algún otro indicador en el nivel precedente, por favor indíquelo a continuación:

_____

_____

_____

	NIVEL DE DEFINICIÓN	SI	NO	NS/NC
1	¿Hay un registro institucional de los procedimientos relacionados con la seguridad de la información?			
2	¿Hay documentos institucionales de las funciones del personal con respecto a la seguridad de la información?			
3	¿Están establecidas en un documento institucional las medidas a tomar en materia de la seguridad de la información?			

4	¿Hay documentos institucionales que establezcan las normas de la seguridad de la información?			
5	¿Están especificados en un documento institucional las obligaciones del usuario no relacionado con la seguridad de la información?			
6	¿Están definidas en documentos institucionales las obligaciones del usuarios que maneja la información crítica del área de la seguridad de la información?			
7	¿Hay registro de los incidentes que afectan la seguridad de la información en la institución?			
8	¿Conocen los empleados de la institución las Políticas de la Seguridad de la Información?			
9	¿Se difunden las Políticas de Confidencialidad de la Información?			
10	¿Se difunden las Políticas de la Integridad de la Información?			
11	¿Se difunden las Políticas de la Disponibilidad de la Información?			
12	¿Se difunden las Políticas de la Autenticidad de la Información?			
13	¿Se difunden las Políticas de la Autorización de la Información?			
14	¿Se difunden las Políticas de las Firmas Electrónicas?			
15	¿Se difunden las Políticas de los Certificados Digitales?			
16	¿Están definidos los valores éticos de la seguridad de la información?			
17	¿Se difunden los valores éticos de la seguridad de la información?			
18	¿Se ofrecen charlas, cursos, seminarios, para el personal de la institución, con el fin de crear cultura de la Seguridad de la Información?			
19	¿En las diversas reuniones inter departamentales se promueve la cultura de la seguridad de la información?			
20	¿Se busca crear conductas que favorezcan los valores éticos, con respecto al manejo de la información?			
21	¿Se promueve la implementación por parte del personal de cada una de las áreas involucradas en el manejo de la información de medidas que contribuyan a mejorarla?			

22	¿Se establecen medidas que induzcan al personal a acatar la normativa existente en materia de la seguridad de la información?			
23	¿Están claramente definidos los roles que en materia de la seguridad de la información juegan cada uno de los involucrados en el manejo de la información institucional?			
24	¿Hay estrategias tendientes a mejorar las falencias en materia de seguridad de la información que permitan trazar un camino a seguir en esta materia?			

Si considera que falta algún otro indicador en el nivel precedente, por favor indíquelo a continuación:

_____

_____

_____

	NIVEL DE GESTIÓN	SI	NO	NS/NC
1	¿Se promueve en la institución el aprendizaje en conjunto de los miembros del equipo de trabajo?			
2	¿Existe una visión compartida entre los miembros de la Unidad a cargo de la Seguridad de la Información			
3	¿Se considera que todos los personales con rango directivo son actores principales en el objetivo de garantizar la seguridad de la información?			
4	¿La institución promueve el desarrollo de capacidades en materia de seguridad de la información, tanto a nivel de gerencia como a niveles medios y de empleado?			
5	¿Se realiza auditoría interna sobre la Seguridad de la Información?			
6	¿Se realiza auditoría externa sobre la Seguridad de la Información?			
7	¿Existe un plan estratégico para garantizar la Seguridad			

	de la Información en la Institución?			
8	¿Se manejan niveles de autorización para que los usuarios puedan acceder a los datos y recursos en el ejercicio diario de sus funciones?			
9	¿Se lleva un control de acceso físico para determinados sitios de la institución, de acuerdo a las funciones del empleado?			
10	¿Es efectiva la gestión del soporte en el área de Seguridad de la Información?			
11	¿Se cumple la Política de Confidencialidad de la Información?			
12	¿Se cumple la Política de Integridad de la Información?			
13	¿Se cumple la Política de la Disponibilidad de la Información?			
14	¿Se cumple la Política en materia de Autenticidad de la Información?			
15	¿Se cumple la Política en materia de Autorización de acceso a los datos?			
16	¿Se cumple la Política de Firmas Electrónicas?			
17	¿Se cumple la Política de Certificados Digitales?			
18	¿Se identifica el personal de la Institución con los valores éticos de la Seguridad de la Información?			
19	¿Se establecen planes para la mejora continua de los niveles de Seguridad de la Información en la Institución?			
20	¿Se discute a alto nivel en la Institución el estado actual de la Seguridad de la Información institucional?			

Si considera que falta algún otro indicador en el nivel precedente, por favor indíquelo a continuación:

	NIVEL Óptimo	SI	NO	NS/NC
1	¿Los cambios o implementaciones en Seguridad de la Información se realizan en equipo?			
2	¿Se realizan actualizaciones y difusión permanente de las Políticas de Seguridad de la Información?			
3	¿Aplica el conjunto de los empleados de la Institución las Políticas de Seguridad de la Información?			
4	¿Existe un criterio uniforme en cuanto a la aplicación de medidas que ayuden a fomentar la Seguridad de la Información?			
5	¿Existe cultura organizacional en materia de la Seguridad de la Información que se pueda considerar institucionalizada?			
6	¿Existe alineación entre las medidas institucionales de salvaguarda con las especificadas en el plan estratégico de Seguridad de la Información?			
7	¿Considera que a todo nivel en la Institución los equipos de trabajo que se conforman comparten la visión en Seguridad de la Información?			
8	¿Forman parte de la cultura institucional los valores éticos de la Seguridad de la Información?			
9	¿Hay alto nivel de formación en materia de Seguridad de la Información en el equipo de trabajo que esta a cargo del área de Seguridad Informática?			
10	¿Hay proactividad en las actuaciones del equipo a cargo de la Seguridad de la Información en la Institución?			
11	¿Se Aplican con frecuencia Metodologías de Análisis y Control de Riesgo?			
12	¿Existe un registro de activos informáticos (Software y Hardware) de la Institución?			
13	¿Existen niveles de comunicaciones entre los equipos de cada una de las áreas informáticas de la institución y el equipo a cargo de la Seguridad de la Información?			
14	¿Se desarrollan en conjunto los planes estratégicos, la implementación de soluciones informáticas y la automatización de procesos con la programación de la			

	Seguridad de la Información?			
15	¿Se realiza un análisis y gestión de riesgo de los nuevos activos incorporados a la institución?			
16	¿Se aplican y desarrollan políticas propias en materia de la Seguridad de la Información?			
17	¿Se cumplen a todos los niveles con las Políticas que le corresponde a cada uno de los usuario de acuerdo a la naturaleza de sus funciones?			
18	¿Esta involucrada toda la Institución en la Seguridad de la Información?			
19	¿Se elaboran campañas destinadas a masificar el conocimiento de las nuevas Políticas de Seguridad de la Información?			

Si considera que falta algún otro indicador en el nivel precedente, por favor indíquelo a continuación:

MODELO DE MADUREZ

Instrucciones: Lea las siguientes interrogantes y conteste de acuerdo a la frecuencia con la que ocurre el evento, tomando en consideración los siguientes valores:

5 Siempre 4 Casi siempre 3 Algunas veces 2 Casi nunca 1 Nunca

	NIVEL DE INICIO	5	4	3	2	1
1	¿Se realizan chequeos de Seguridad de la Información de Manera periódica?					
2	¿Los incidentes asociados a la Seguridad de la Información conducen a impacto de consideración con que frecuencia?					

	NIVEL DE RECONOCIMIENTO	5	4	3	2	1
1	¿Se revisa de manera cotidiana el tema de la Seguridad de la Información, en las diversas áreas?					
2	¿Con que frecuencia el impacto de los incidentes de seguridad tienen consecuencias de máximo impacto?					
3	¿Con que frecuencia se definen las responsabilidades en materia de seguridad de la información					
4	¿Con que frecuencia se pierden los esfuerzos en materia de seguridad de la información, que son implementados en la plataforma institucional?					

	NIVEL DE DEFINICIÓN	5	4	3	2	1
1	¿La plataforma tecnológica de la institución se actualiza de manera periódica?					

2	¿La plataforma cuenta con soluciones antivirus, antiespias, anti SPAM y otros anti Malware, que en caso de ser licenciados son actualizados una vez que llega al termino la duración de las licencias?					
3	¿Se realiza un monitoreo para evaluar el comportamiento de la red de manera cotidiana?					
4	¿Se llevan estadísticas y bitácoras que registren el comportamiento de la red?					
5	¿Se realizan respaldos de todos los activos críticos de la plataforma?					
6	¿Se debe contar con autorización para el acceso a los aplicativos, equipos y demás recursos para que los usuarios cumplan con sus funciones?					
7	¿El acceso físico a las áreas críticas de la institución es registrado regularmente?					

	NIVEL DE GESTIÓN	5	4	3	2	1
1	¿La institución tiene un registro detallado de los incidentes de seguridad?					
2	¿Tiene la institución registro automatizado de los eventos que puedan comprometer la seguridad informática de la plataforma?					
3	¿Hay difusión masiva de los planes en materia de seguridad informática?					
4	¿El trabajo en materia de seguridad informática se maneja al mas alto nivel en la institución?					
5	¿Están definidos los valores éticos de la Seguridad de la Información?					
6	¿Hay difusión masiva de los valores éticos de la Seguridad de la Información?					
7	¿Se ofrecen al personal directivo charlas, cursos, seminarios, con la finalidad de crear cultura organizacional en materia de seguridad de la información?					
8	Se ofrecen al personal no directivo charlas, cursos, seminarios, con la finalidad de crear cultura organizacional en materia de seguridad					

	de la información?					
9	¿Se ofrecen al personal técnico en el área de informática charlas, cursos, seminario, con la finalidad de crear cultura organizacional en materia de seguridad de la información?					
10	¿En las reuniones entre los distintos departamentos se fomenta la creación de cultura organizacional, en materia de Seguridad de la Información?					
11	¿Se fomenta la formación de hábitos que promuevan los valores éticos, con respecto al manejo de la información?					
12	¿Se maneja a todo nivel los servicios de confidencialidad, integridad, autenticidad, autorización y disponibilidad de la información?					
13	¿Se tiene un control del valor de los activos de la institución?					
14	¿Se mantiene actualizado el valor de los activos institucionales?					

	NIVEL ÓPTIMO	5	4	3	2	1
1	¿La toma de decisiones en materia de seguridad de la información cuenta con el apoyo de las máximas autoridades de la institución?					
2	¿La gestión de la seguridad de la información lleva un control de eventos?					
3	¿La difusión de las Políticas de Información se realiza a todos los niveles del personal?					
4	¿El Soporte del área de a Seguridad Informática es medido para conocer la efectividad de dicha tarea?					
5	¿Se toman decisiones en el área de la Seguridad Informática en función de los registros de incidentes y demás eventos en el área?					
6	¿Se maneja a todo nivel los servicios de confidencialidad, integridad, autenticidad, autorización y disponibilidad de la información?					

7	¿El personal de la institución esta identificado con los valores de Seguridad de la Información?					
8	¿Se mantienen actualizadas las Políticas de Seguridad de la Información en la Institución?					
9	¿Hay Metodología de Seguridad de la Información que dicte los patrones a seguir en la materia?					

Muy agradecido por la colaboración prestada en el desarrollo del presente trabajo de investigación.

ANEXO B

LOCALIDADES DEL IVSS

REGIÓN	LOCALIDAD	ESTADO	CIUDAD
CENTRAL	Oficina Administrativa Maracay	Aragua	Maracay
	Oficina Administrativa Carabobo (Valencia)	Carabobo	Valencia
	Oficina Administrativa Puerto Cabello	Carabobo	Puerto Cabello
	Hospital José María Carabaño Tosta	Aragua	Maracay
	Hospital José Antonio Vargas (PALO NEGRO)	Aragua	Palo Negro
	Hospital Ángel Larralde	Carabobo	Valencia
	Hospital Molina Sierra	Carabobo	Puerto Cabello
	Oficina Administrativa San Carlos	Cojedes	San Carlos
	Oficina Administrativa La Victoria	Aragua	La Victoria
	Oficina Administrativa Cagua	Aragua	Cagua
	Ambulatorio Emiliano Azcunez	Carabobo	Valencia
	Ambulatorio Yagua	Carabobo	Guacara
	Ambulatorio Luis Izaguirre	Carabobo	Mariara
	Ambulatorio Luis Rodriguez Panacci	Carabobo	San Joaquín

	Ambulatorio Morón	Carabobo	Morón
	Ambulatorio Santa Rosa	Carabobo	Puerto Cabello
	Ambulatorio Tocuyito Bélgica Tovar (REMODELACION)	Carabobo	Tocuyito
	Ambulatorio Tinaquillo	Cojedes	Tinaquillo
	Ambulatorio El Limón	Aragua	El Limón
	Ambulatorio Negra Matea	Aragua	Maracay
	Ambulatorio San Carlos	Cojedes	San Carlos
	Ambulatorio Francisco Chico Matos	Aragua	Cagua
	Ambulatorio Luis Richard Diaz	Aragua	La Vitoria
	Ambulatorio Luis Guada Lacau	Carabobo	Valencia
	Ambulatorio Paraparal	Carabobo	Los Guayos
CAPITAL	Oficina Administrativa Del Distrito Federal (Parque Central)	Capital	Caracas
	Oficina Administrativa La Guaira (BT)	Vargas	La Guaira
	Oficina Administrativa Chacao	Capital	Caracas
	Oficina Administrativa Mata Linda (BT)	Miranda	Valles del Tuy
	Oficina Administrativa Guarenas	Miranda	Guarenas
	Oficina Administrativa Los Teques	Miranda	Los Teques
	Ambulatorio Naiguatá	Vargas	Naiguatá

	Ambulatorio José Gonzalez Navarro	Miranda	Caracas – La Trinidad
	Ambulatorio Cua	Miranda	Cua
	Proveeduría Caricuao	Capital	Caracas
	Ambulatorio Julio de Armas	Miranda	Valles del Tuy
	Especialidades Medicas Horacio Almeida	Capital	Caracas
	Unidad de Inmunología Clínica San Bernardino	Capital	Caracas
	Ambulatorio Los Cortijos de Lourdes	Miranda	Caracas
	Ambulatorio Centro Médico Dr. Dilio Sequera Peraza	Capital	Caracas
	Ambulatorio Armando Castillo Plaza	Capital	Caracas
	Unidad Nacional de Psiquiatría Infantil Alecia Peña		
	Ambulatorio Julio Iribarren Borges	Capital	Caracas
	Ambulatorio Carlos Diez del Ciervo	Miranda	Caracas
	Ambulatorio Ángel Vicente Ochoa	Capital	Caracas
	Ambulatorio Germán Quintero	Miranda	Los Teques
	Hospital José Gregorio Hernández	Capital	Caracas
	Hospital Elías Toro	Capital	Caracas

	Clínica Maternidad Santa Ana	Capital	Caracas
	Hospital Dr. Luis Salazar Dominguez	Miranda	Guarenas
	Hospital José María Vargas	Vargas	La Guaira
	Centro Nacional de Rehabilitación Dr Alejandro Rhode	Capital	Caracas
	Hospital Miguel Pérez Carreño	Capital	Caracas
	Consulta Externa (PÉREZ CARREÑO)	Capital	Caracas
	Hospital Domingo Luciani	Capital	Caracas
	Clínica Popular del Valle Dr Patrocinio Peñuela Ruiz	Capital	Caracas
	Clínica Popular Lebrum Jesús Yerena	Capital	Caracas
	Clínica Popular de Catia Dr Pedro Felipe Arreaza Calatrava	Capital	Caracas
	Clínica Popular del Paraíso Dr Francisco Salazar MeneseS	Capital	Caracas
	Clínica Popular Caricuao	Capital	Caracas
	Centro Oftalmológico Misión Milagro de Vargas	Vargas	La Guaira
	Torre Norte CSB (CENTRO SIMON Bolívar)	Capital	Caracas
	Torre Domus (Fiscalización)	Capital	Caracas
	Centro Abastecimiento (Almacen) Guatire	Miranda	Guatire

	Centro de Almacenamiento Ocumare	Miranda	Ocumare
	Dirección General de Perdida Involuntaria del Empleo (SAPPIE)	Miranda	Caracas
	Farmacia Medicamentos de Alto Costo	Miranda	Caracas
	Hospital Oncológico Padre Machado	Capital	Caracas
	Psiquiátrico Jesús Mata De Gregorio (Los Chorros)	Miranda	Caracas
	Centro de Almacenamiento Carapa	Caracas	Capital
	Centro de Abastecimiento y Distribucion Caucagua (Centro de Convenciones) (BT)	Miranda	Caucagua
	Dirección Logística San Martín	Capital	Caracas
	Dirección General Ingeniería (San Bernardino)	Capital	Caracas
	Ambulatorio Los Roques (BT)	Miranda	Los Roques
	Oficina Administrativa Guarenas-Ban Valor (REMODELACION)	Miranda	Guarenas
	Oficina Administrativa El Paraíso	Capital	Caracas
	Oficina Administrativa Puerto La Cruz	Anzoategui	Puerto la Cruz
	Ambulatorio Carlos Marti Buffil	Anzoategui	Puerto laCruz

ORIENTAL	Ambulatorio Hector Farias	Anzoategui	El Tigre
	Ambulatorio José María Vargas (REDESCOM)	Nueva Esparta	Porlamar
	Ambulatorio Hector Farias	Anzoategui	El Tigre
	Oficina Administrativa Anaco	Anzoategui	Anaco
	Oficina Administrativa Maturin	Monagas	Maturin
	Oficina Administrativa Cumana	Sucre	Cumana
	Oficina Administrativa Carupano	Sucre	Carupano
	Oficina Administrativa Punta de Mata (BT)	Monagas	Punta de Mata
	Hospital César Rodriguez	Anzoategui	Puerto la Cruz
	Hospital Luis Ortega	Nueva Esparta	Porlamar
	Hospital Guzmán Lander	Anzoategui	Barcelona
	Farmacia Medicamentos de Alto Costo	Sucre	Cumana
	Guarderia Doña Barbara Mendez	Anzoategui	Pto la Cruz
	Ambulatorio Maturin	Monagas	Maturin
	Oficina Administrativa El Tigre	Anzoategui	El Tigre
	Oficina Administrativa Bolívar	Bolívar	Ciudad Bolívar
	Ambulatorio Lino Maradei Donato	Bolívar	Ciudad Bolívar
	Centro de Rehabilitación Carlos Fragachan	Bolívar	Pto Ordaz
	Ambulatorio Roberto Lozano Villegas (REDESCOM)	Bolívar	San Felix

GUAYANA	Ambulatorio Renato Valera Aguirre (REDESCOM)	Bolívar	Pto. Ordaz
	Ambulatorio Vinicio Grillet Maurera	Bolívar	San Felix
	Ambulatorio Luis Guillermo Perozo	Bolívar	Pto. Ordaz
	Ambulatorio César Bello - Upata	Bolívar	Upata
	Hospital Raúl Leoni	Bolívar	San Felix
	Hospital Uyapar	Bolívar	Pto. Ordaz
	Hospital Nouel Joubert	Bolívar	Ciudad Bolívar
	Hospital Juan Germán Rocío	Bolívar	El Callao
	Oficina Administrativa Upata	Bolívar	Upata
	Oficina Administrativa El Callao	Bolívar	El Callao
	Oficina Administrativa Puerto Ayacucho	Amazonas	Pto Ayacucho
	Oficina Administrativa Tucupita	Delta Amacuro	Tucupita
	Oficina Administrativa Sur Oriental (Puerto Ordaz)	Bolívar	Pto. Ordaz
	Oficina Administrativa Maracaibo	Zulia	Maracaibo
	Ambulatorio Sur Veritas (Maracaibo)	Zulia	Maracaibo
	Ambulatorio Ciudad Ojeda	Zulia	Ciudad Ojeda
	Ambulatorio La Concepción	Zulia	Maracaibo
	Ambulatorio Centro Norte	Zulia	Maracaibo

ZULIANA	Ambulatorio Sabaneta	Zulia	Sabaneta
	Ambulatorio Santa Rita	Zulia	Santa Rita
	Ambulatorio Cabimas (REDESCOMM)	Zulia	Cabimas
	Hospital Adolfo Pons	Zulia	Maracaibo
	Hospital Pedro Garcia Clara	Zulia	Ciudad Ojeda
	Hospital Noriega Trigo	Zulia	San Francisco
	Oficina Administrativa Ciudad Ojeda	Zulia	Maracaibo
	Oficina Administrativa Santa Barbara	Zulia	Santa Barbara
	Oficina Administrativa Cabimas (BT)	Zulia	Cabi
OCCIDENTAL	Oficina Administrativa Barquisimeto	Lara	Barquisimeto
	Oficina Administrativa Punto Fijo	Falcón	Punto Fijo
	Ambulatorio Chivacoa	Yaracuy	Chivacoa
	Ambulatorio Punto Fijo	Falcón	Punto Fijo
	Ambulatorio Rafael Vicente Andrade	Lara	Barquisimeto
	Hospital Rafael Calles Sierra	Falcón	Punto Fijo
	Hospital Pastor Oropeza Riera	Lara	Barquisimeto
	Hospital Cardón	Falcón	Punta Cardon
	Hospital Jesús Garcia Coello	Falcón	Punto Fijo
	Hospital Rafael Gallardo	Falcón	Coro

	Hospital Juan Daza Pereira	Lara	Barquisimeto
	Oficina Administrativa Coro (FALCON)	Falcón	Coro
	Oficina Administrativa Carora	Lara	Carora
	Oficina Administrativa San Felipe	Yaracuy	San Felipe
	Administrativa Santa Rosa (Barquisimeto)	Lara	Barquisimeto
ANDINA	Oficina Administrativa San Antonio (San Cristóbal)	Tachira	San Cristobal
	Oficina Administrativa Valera	Trujillo	Valera
	Oficina Administrativa Mérida	Mérida	Mérida
	Ambulatorio Romero Lobo	Tachira	La Fria
	Ambulatorio Nuestra Señora de la Paz	Trujillo	Valera
	Hospital Trujillo	Trujillo	Trujillo
	Ambulatorio Valera	Trujillo	Valera
	Hospital Tulio Carnavalli Salvatierra	Mérida	Mérida
	Hospital Juan Montezuma Ginnari (BT)	Trujillo	Valera
	Hospital Patrocinio Peñuela Ruiz	Tachira	San Cristobal
	Oficina Administrativa Bocono	Trujillo	Boconó
	Oficina Administrativa El Vigía	Mérida	El Vigia
	Oficina Administrativa Trujillo	Trujillo	Trujillo

	Ambulatorio Tiscachi	Trujillo	Boconó
LOS LLANOS	Oficina Administrativa Apure	Apure	Apure
	Oficina Administrativa Barinas (BT)	Barinas	Barinas
	Ambulatorio Emilio Carmona Gomez -Barinas	Barinas	Barinas
	Ambulatorio San Fernando de Apure (REMODELACION)	Apure	San Fernando
	Oficina Administrativa Acarigua	Portuguesa	Acarigua
	Oficina Administrativa Guanare	Portuguesa	Guanare
	Centro Materno José Gregorio Hernández	Portuguesa	Guanare
	Unidad Bolívariana de Nefrología y Diálisis del Hosp. Luis Razetti	Barinas	Barinas
	Oficina Administrativa San Juan de los Morros	Guarico	San Juan de los Morros
	Ambulatorio San Juan de los Morros	Guarico	San Juan de los Morros
	Ambulatorio Calabozo (REDESCOM)	Guarico	Calabozo
	Oficina Administrativa Valle La Pascua	Guarico	Valle de la Pascua

Fuente: Elaboración Propia (2016)

ANEXO C

Resultados del cuestionario exploratorio Nivel Inicio

1) ¿Existe un departamento encargado de la Seguridad Informática en la Institución?

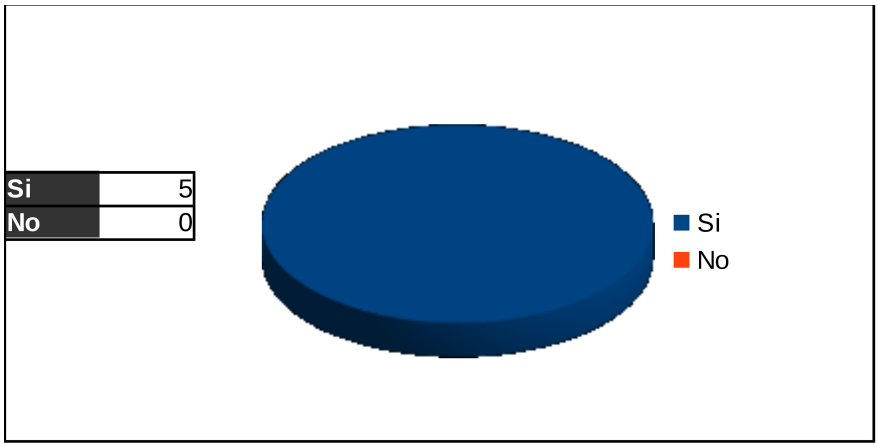

Figura 13: Respuesta item 1 Inicio

Fuente: Elaboración propia.

Nivel de reconocimiento

1)¿Existe una persona encargada de la Seguridad de la Información?

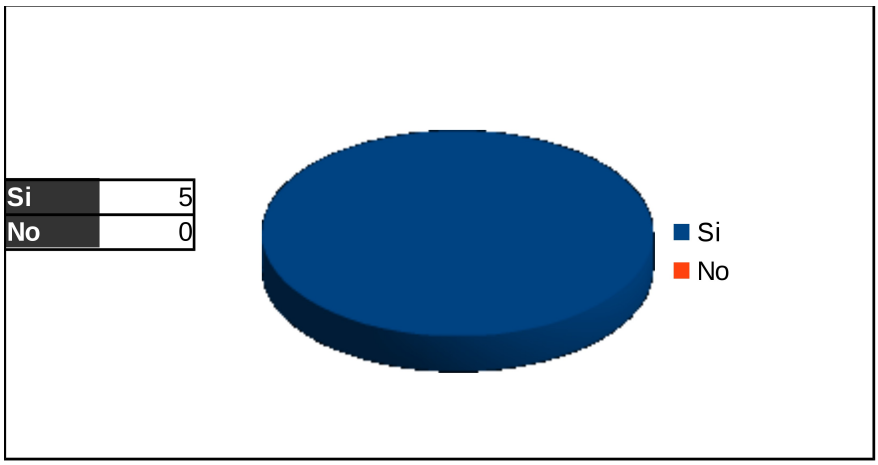

Figura 14: Respuesta item 1Reconocimiento. Fuente: Elaboración propia.

2)¿Las personas que conforman el departamento encargado de la Seguridad Informática son del área Informática?

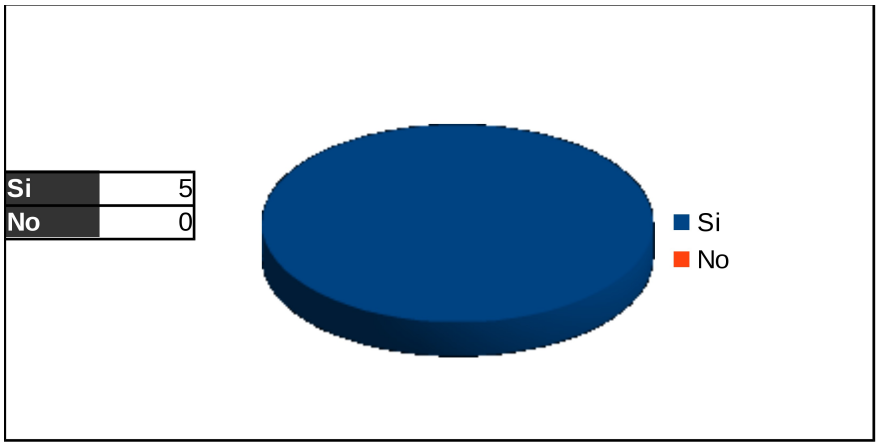

Figura 15: Respuesta item 2 Reconocimiento

Fuente: Elaboración propia.

3)¿Las personas que laboran en el departamento tienen experiencia en el área?

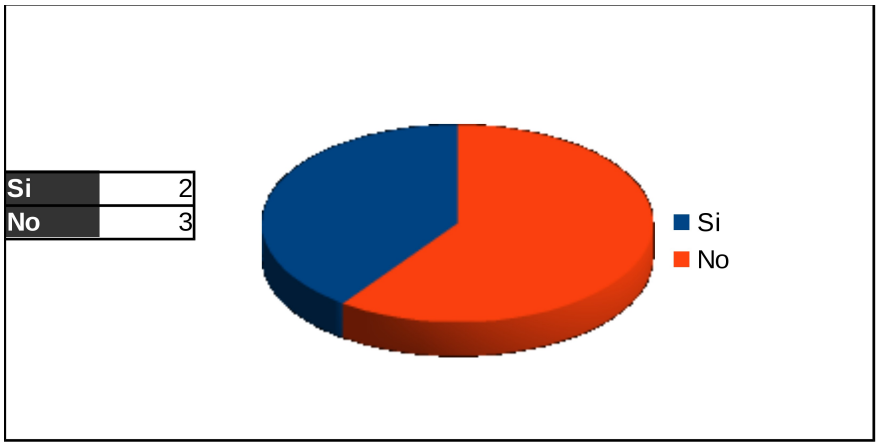

Figura 16: Respuesta item 3 Reconocimiento

Fuente: Elaboración propia.

4)¿Hay herramientas de seguridad como antivirus en la plataforma institucional?

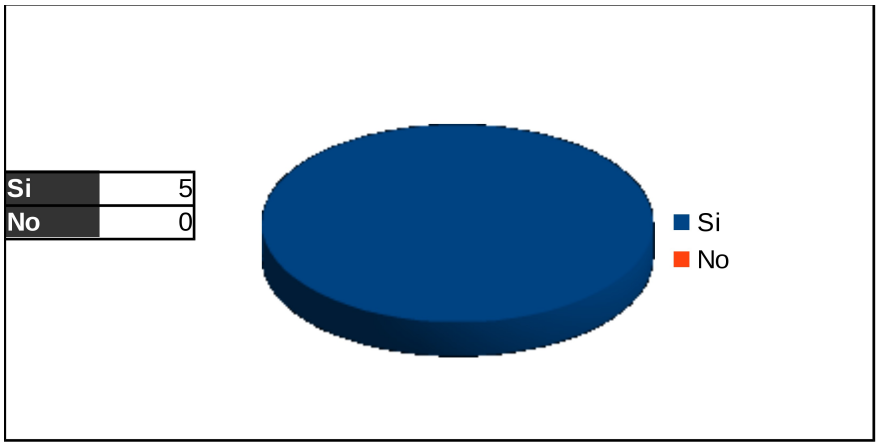

Figura 17: Respuesta item 4 Reconocimiento

Fuente: Elaboración propia.

5)¿Hay herramientas de seguridad como detector de intrusos en la plataforma institucional?

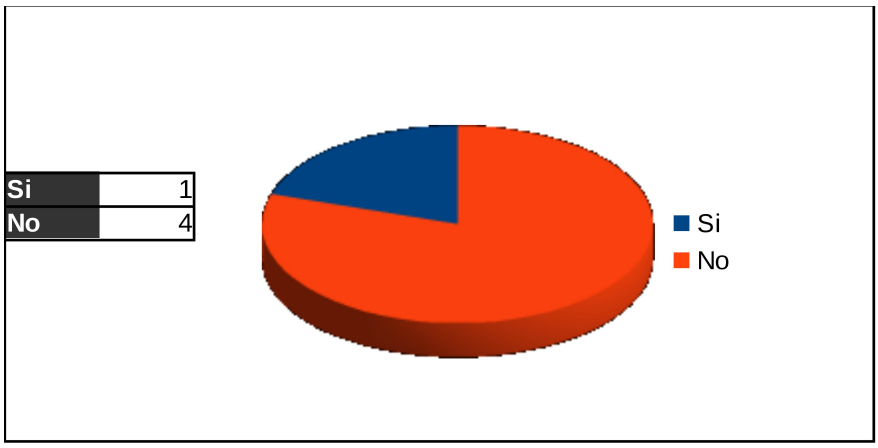

Figura 18: Respuesta item 5 Reconocimiento

Fuente: Elaboración propia.

6)¿Hay herramientas de seguridad como proxies en la plataforma institucional?

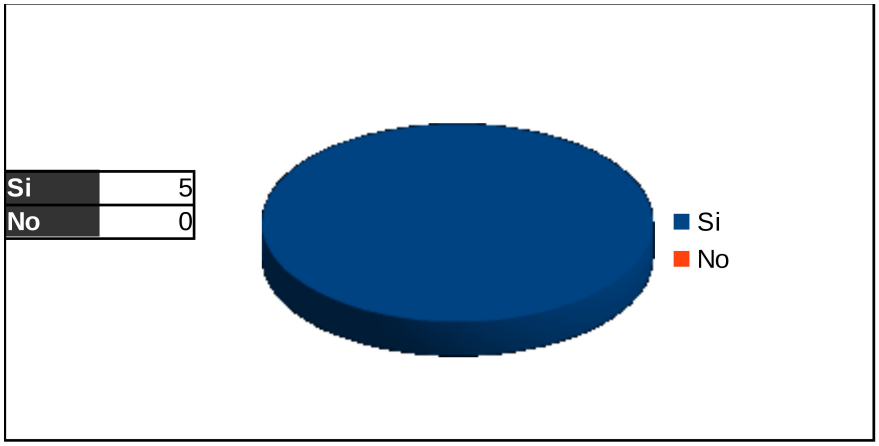

Figura 19: Respuesta item 6 Reconocimiento

Fuente: Elaboración propia.

7)¿Tiene la plataforma institucional herramientas como firewall de sotfware?

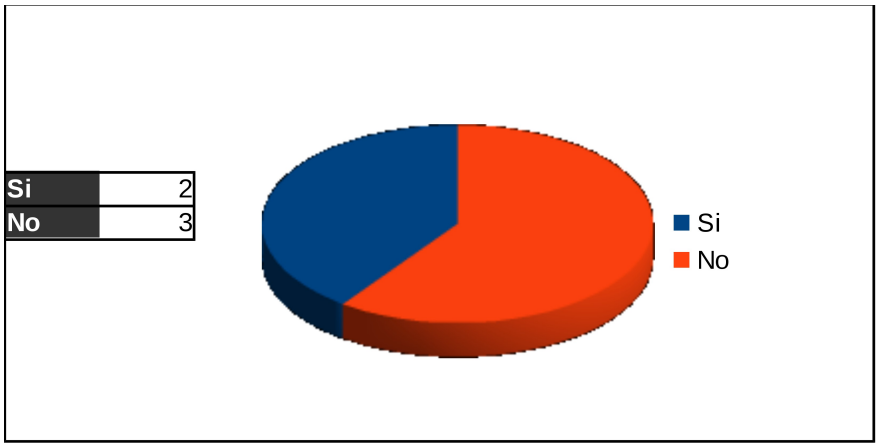

Figura 20: Respuesta item 7 Reconocimiento

Fuente: Elaboración propia.

8)¿Tiene la plataforma institucional herramientas como firewall de hardware?

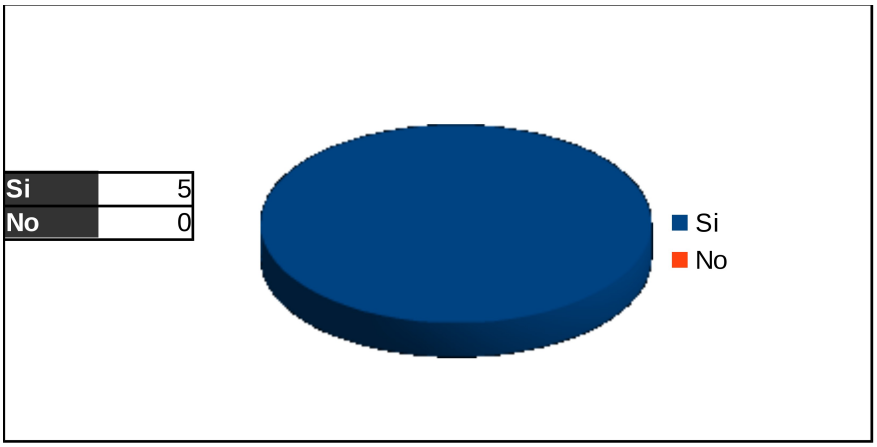

Figura 21: Respuesta item 8 Reconocimiento

Fuente: Elaboración propia.

9)¿Tiene instalada en la plataforma institucional alguna herramienta de software antiespias?

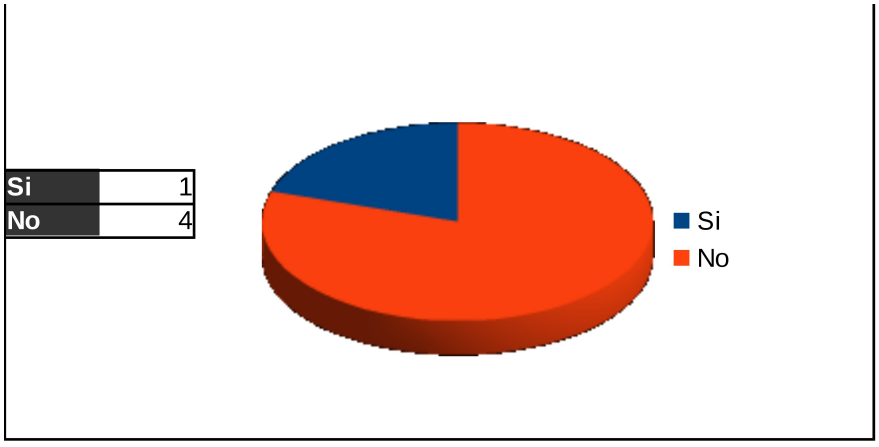

Figura 22: Respuesta item 9 Reconocimiento

Fuente: Elaboración propia.

10)¿Hay un departamento encargado de la seguridad física de la información en la institución?

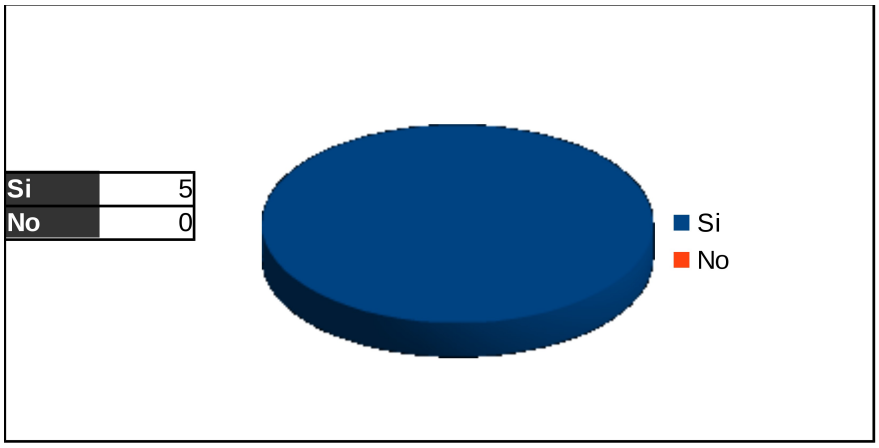

Figura 23: Respuesta item 10 Reconocimiento

Fuente: Elaboración propia.

11)¿Existen políticas de seguridad que determinen la responsabilidad de la aplicación de medidas de seguridad en la Institución?

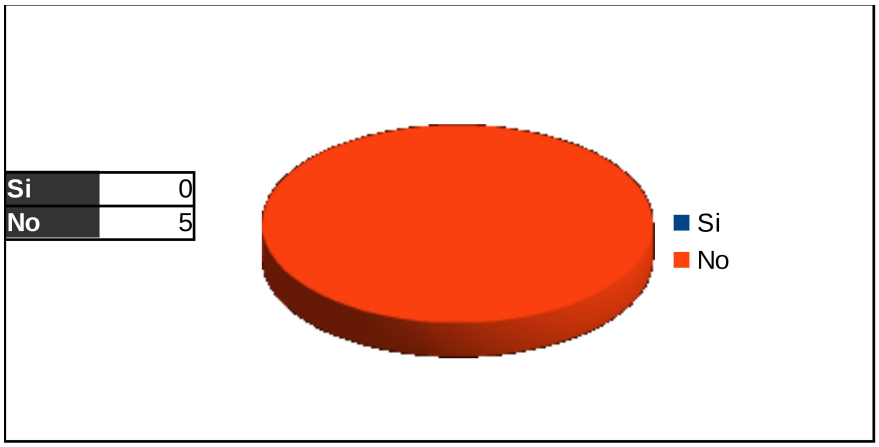

Figura 24: Respuesta item 11 Reconocimiento

Fuente: Elaboración propia.

12)¿Tiene la institución instalada herramientas que permitan conocer el estado del tráfico de redes en la institución?

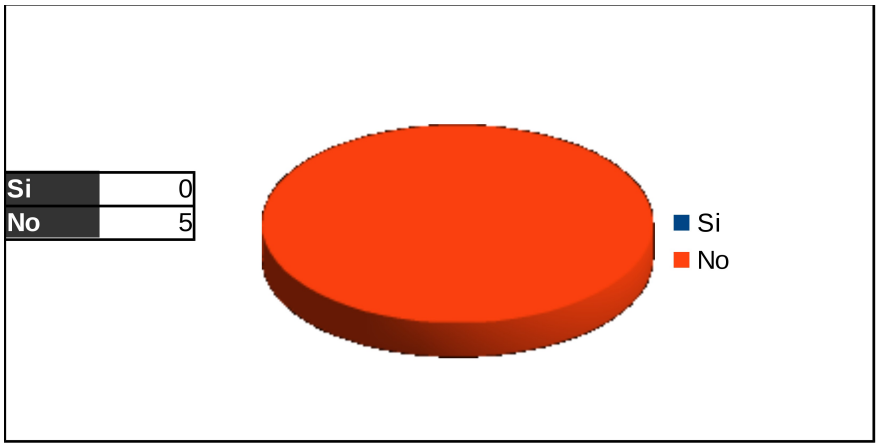

Figura 25: Respuesta item 12 Reconocimiento

Fuente: Elaboración propia.

13)¿Existe un marco de trabajo de la Seguridad de la Información en la institución?

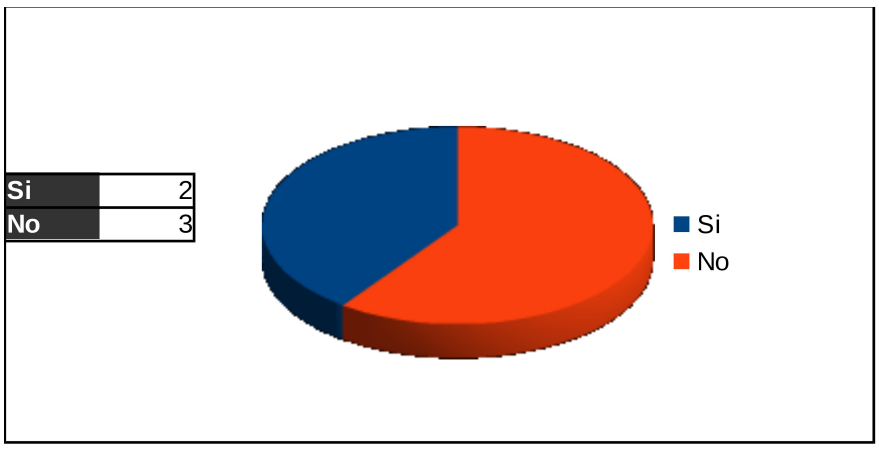

Figura 26: Respuesta item 13 Reconocimiento

Fuente: Elaboración propia.

14)¿Los programas instalados en las aplicaciones son actualizados regularmente?

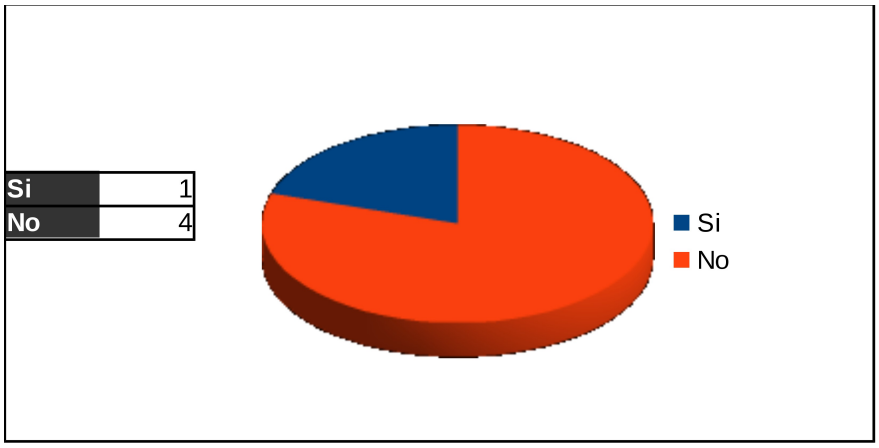

Figura 27: Respuesta item 14 Reconocimiento

Fuente: Elaboración propia.

15)¿Existe un marco de trabajo de la Seguridad de la Información en la institución?

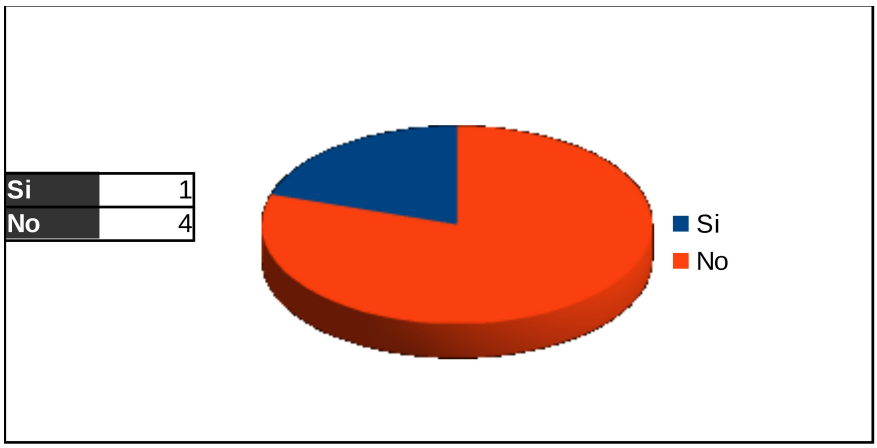

Figura 28: Respuesta item 15 Reconocimiento

Fuente: Elaboración propia.

16) ¿Los programas instalados en las aplicaciones son actualizados regularmente?

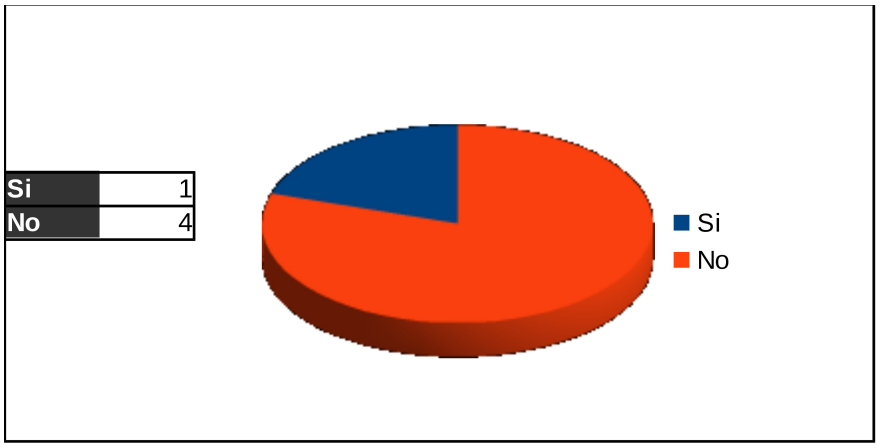

Figura 29: Respuesta item 16 Reconocimiento

Fuente: Elaboración propia.

17)¿Se realizan copias de respaldo y recuperación de datos en la institución con regularidad y niveles de retención?

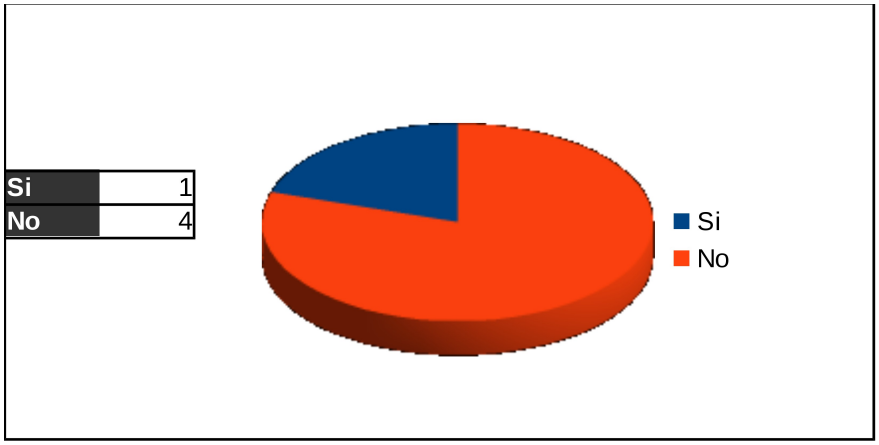

Figura 30: Respuesta item 17 Reconocimiento

Fuente: Elaboración propia.

Nivel definición

1)¿Hay un registro institucional de los procedimientos relacionados con la seguridad de la información?

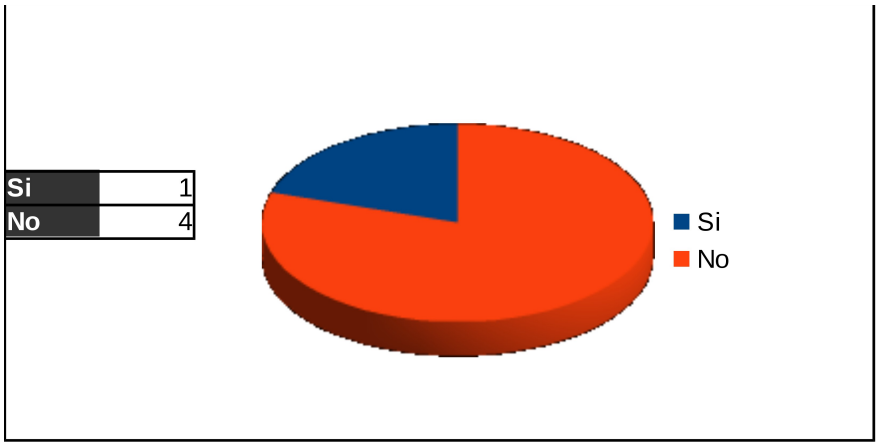

Figura 31: Respuesta item 1 Definición

Fuente: Elaboración propia.

2)¿Hay documentos institucionales de las funciones del personal con respecto a la seguridad de la información?

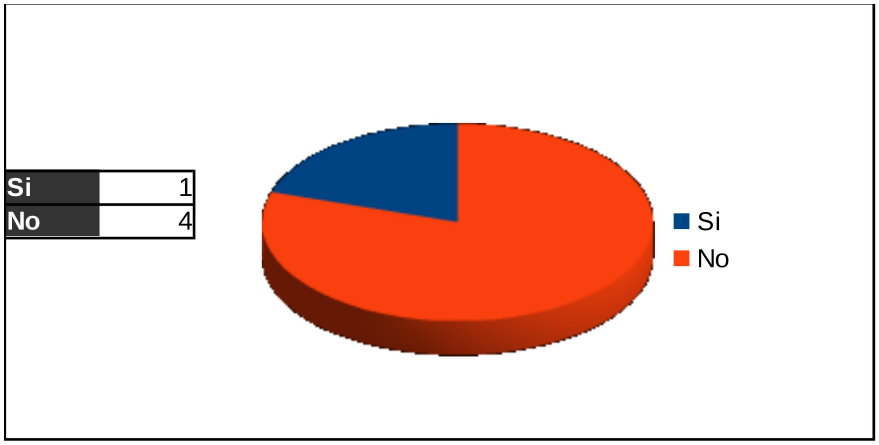

Figura 32: Respuesta item 2 Definición

Fuente: Elaboración propia.

3)¿Están establecidas en un documento institucional las medidas a tomar en materia de la seguridad de la información?

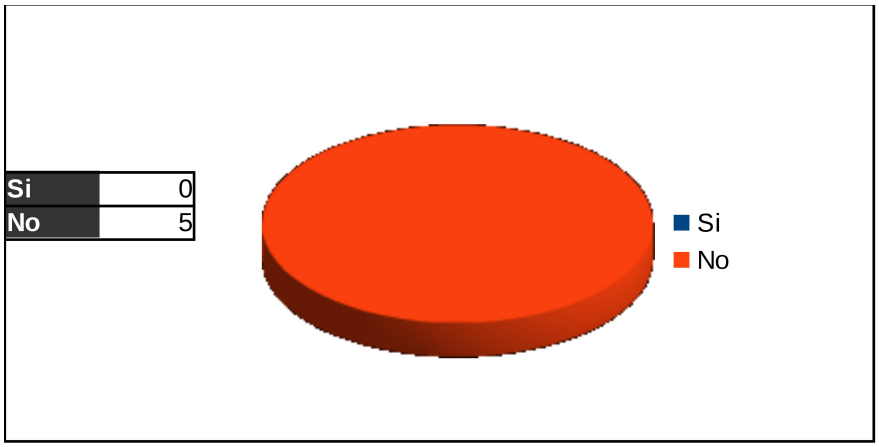

Figura 33: Respuesta item 3 Definición

Fuente: Elaboración propia.

4)¿Hay documentos institucionales que establezcan las normas de la seguridad de la información?

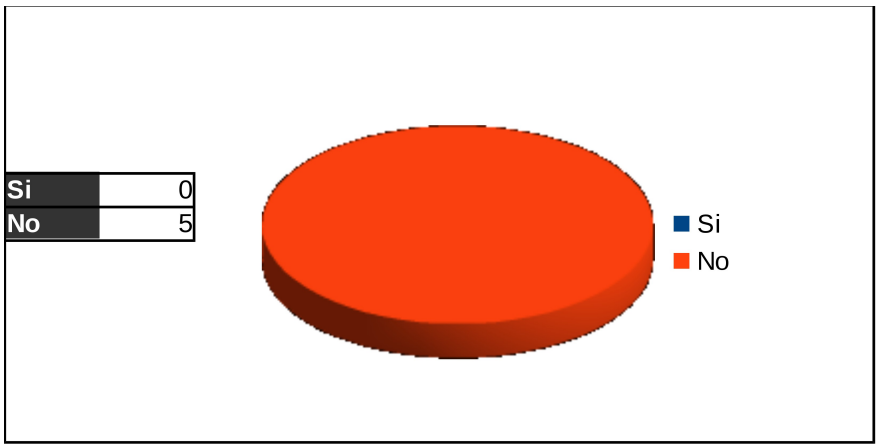

Figura 34: Respuesta item 4 Definición

Fuente: Elaboración propia.

5)¿Están especificados en un documento institucional las obligaciones del usuario no relacionado con la seguridad de la información?

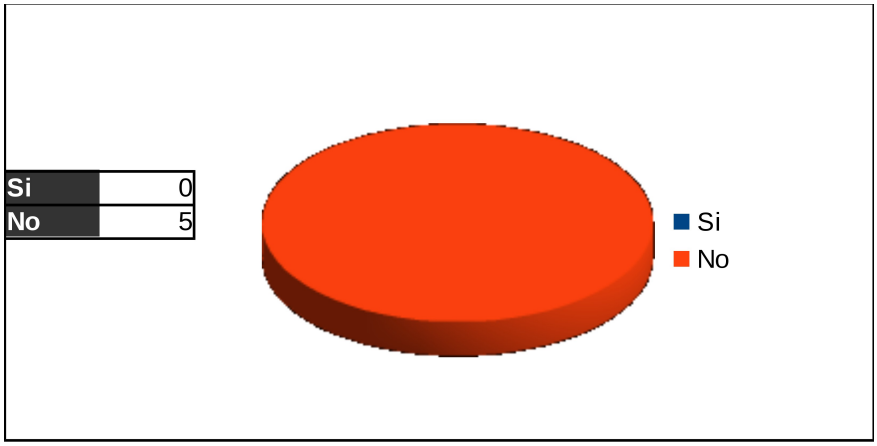

Figura 35: Respuesta item 5 Definición

Fuente: Elaboración propia.

6)¿Están definidas en documentos institucionales las obligaciones de usuarios que manejan la información crítica del área de la seguridad de la información?

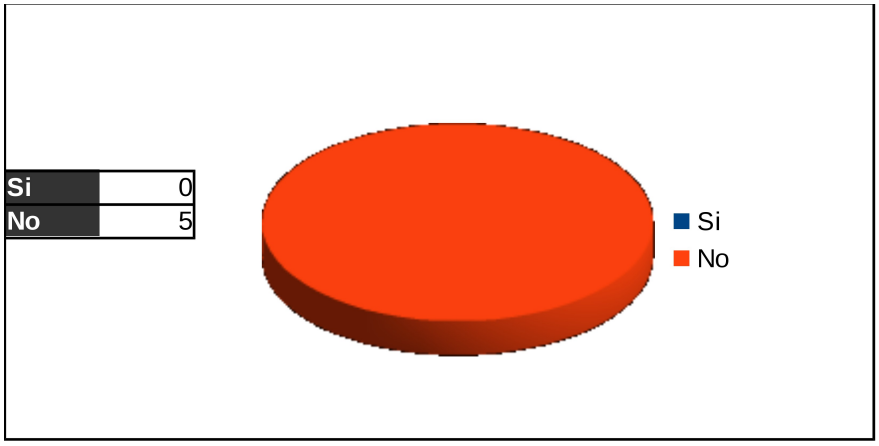

Figura 36: Respuesta item 6 Definición

Fuente: Elaboración propia.

7)¿Hay registro de los incidentes que afectan la seguridad de la información en la institución?

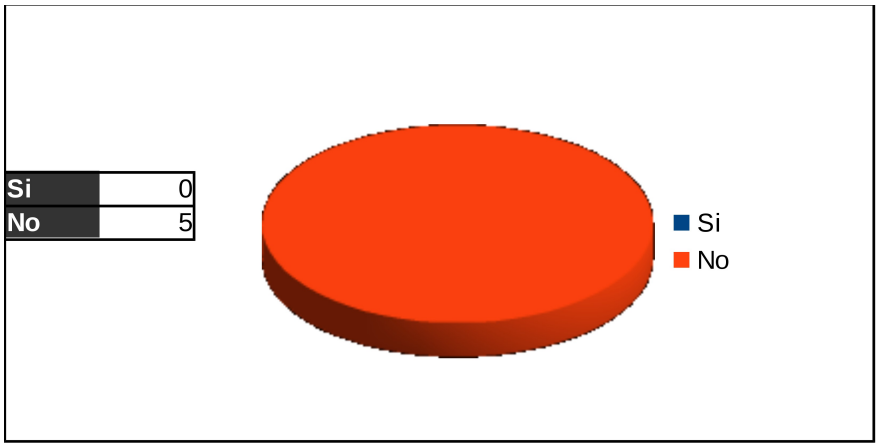

Figura 37: Respuesta item 7 Definición

Fuente: Elaboración propia.

8)¿Conocen los empleados de la institución las Políticas de la Seguridad de la Información?

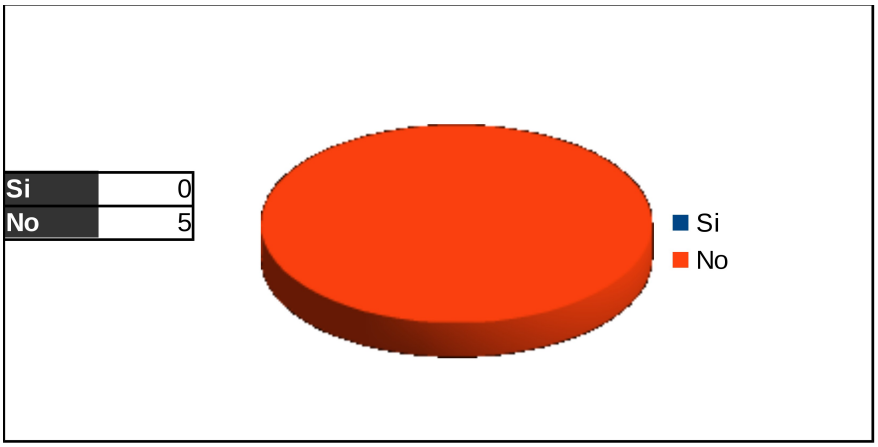

Figura 38: Respuesta item 8 Definición

Fuente: Elaboración propia.

9)¿Se difunden las Políticas de Confidencialidad de la Información?

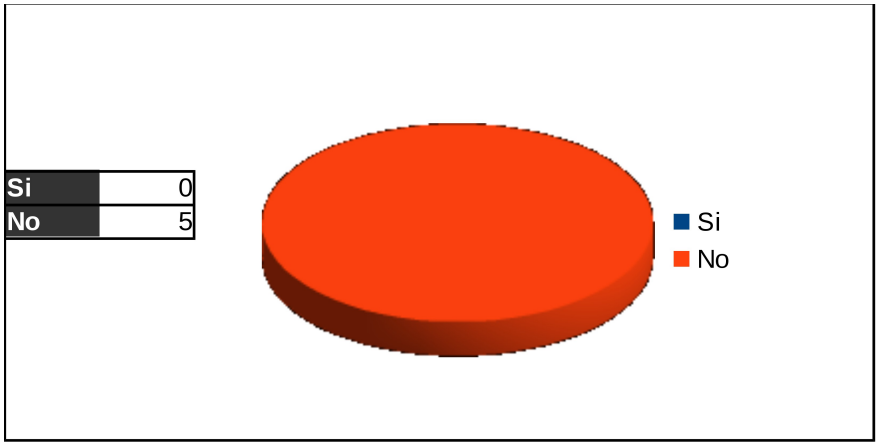

Figura 39: Respuesta item 9 Definición

Fuente: Elaboración propia.

10)¿Se difunden las Políticas de la Integridad de la Información?

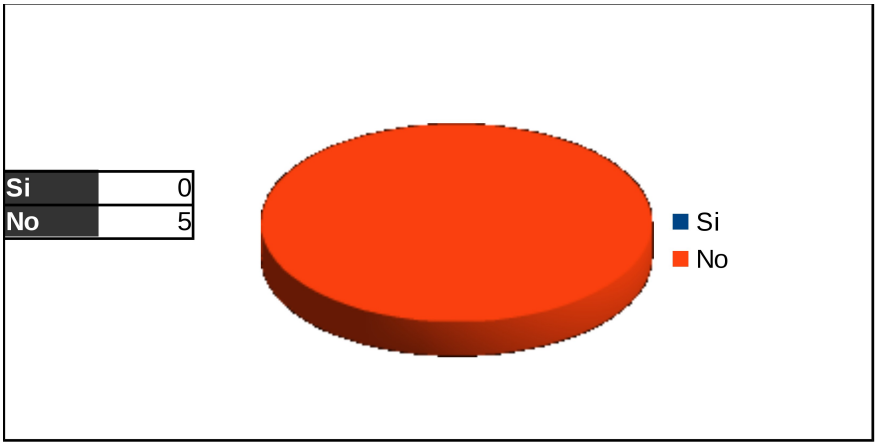

Figura 40: Respuesta item 10 Definición

Fuente: Elaboración propia.

11)¿Se difunden las Políticas de la Disponibilidad de la Información?

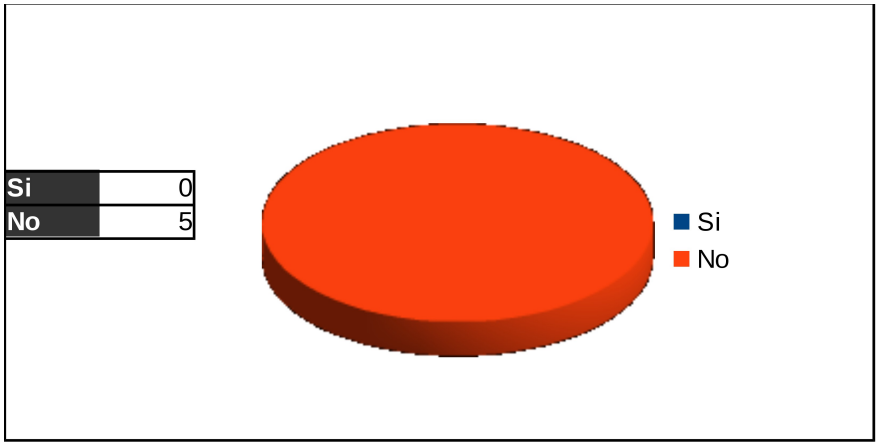

Figura 41: Respuesta item 11 Definición

Fuente: Elaboración propia.

12)¿Se difunden las Políticas de la Autenticidad de la Información?

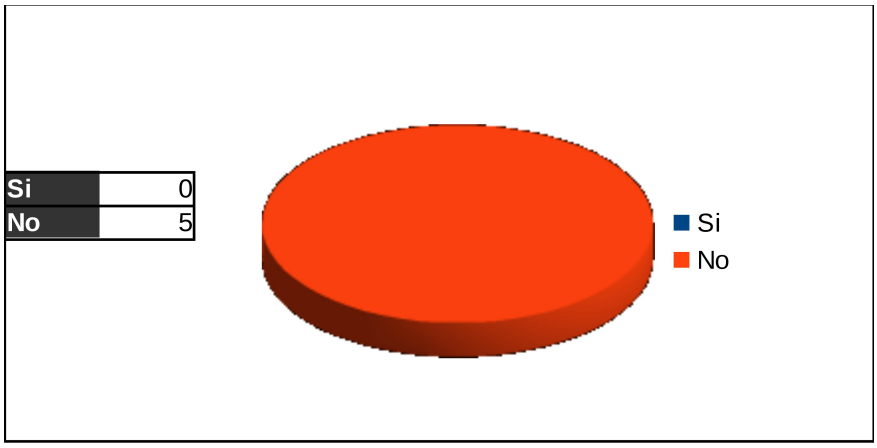

Figura 42: Respuesta item 12 Definición

Fuente: Elaboración propia.

13)¿Se difunden las Políticas de la Autorización de la Información?

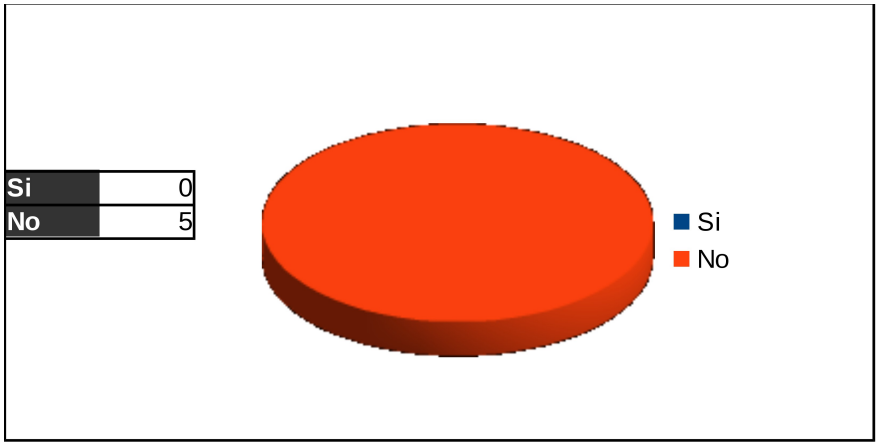

Figura 43: Respuesta item 13 Definición

Fuente: Elaboración propia.

14)¿Se difunden las Políticas de las Firmas Electrónicas?

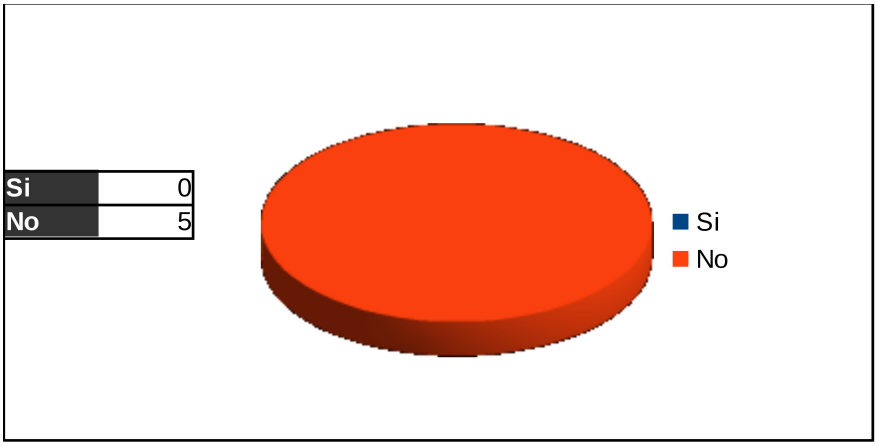

Figura 44: Respuesta item 14 Definición

Fuente: Elaboración propia.

15)¿Se difunden las Políticas de los Certificados Digitales?

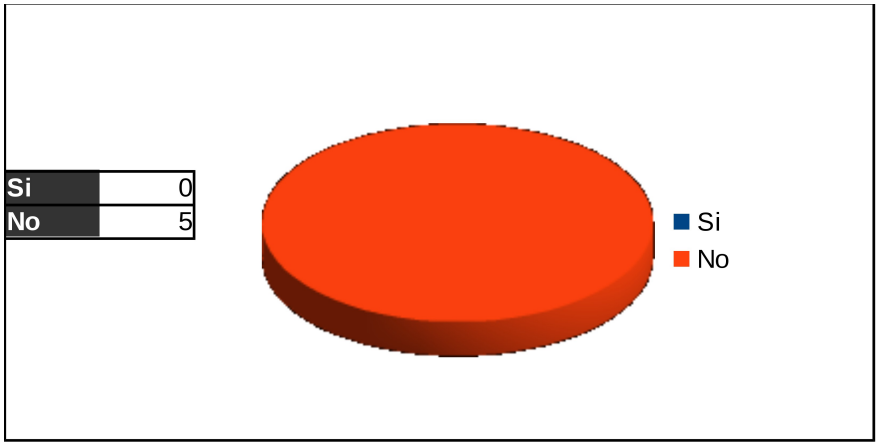

Figura 45: Respuesta item 15 Definición

Fuente: Elaboración propia.

16)¿Están definidos los valores éticos de la seguridad de la información?

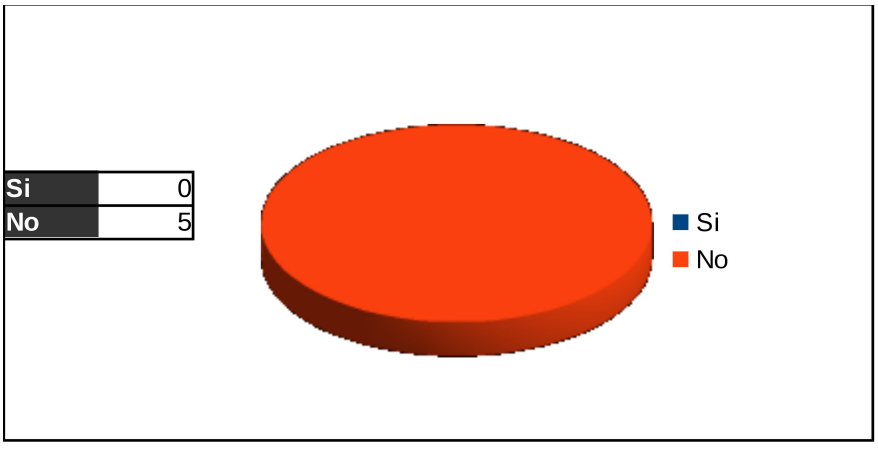

Figura 46: Respuesta item 16 Definición

Fuente: Elaboración propia.

17)¿Se difunden los valores éticos de la seguridad de la información?

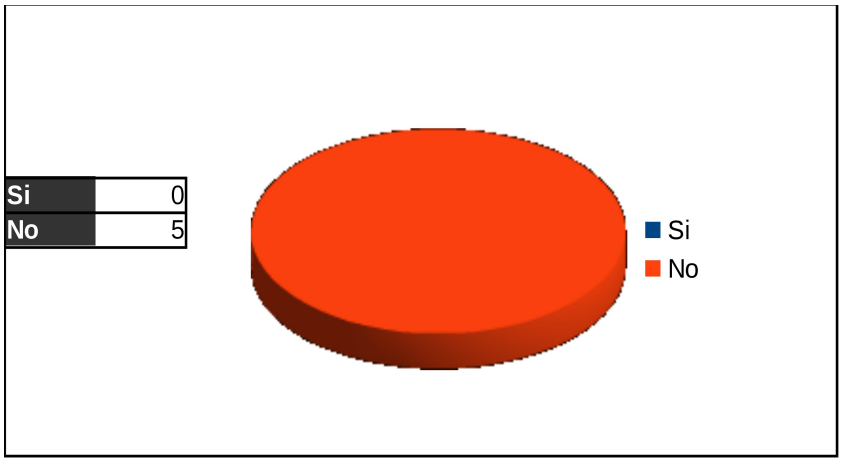

Figura 47: Respuesta item 17 Definición

Fuente: Elaboración propia.

18)¿En las diversas reuniones inter departamentales se promueve la cultura de la seguridad de la información?

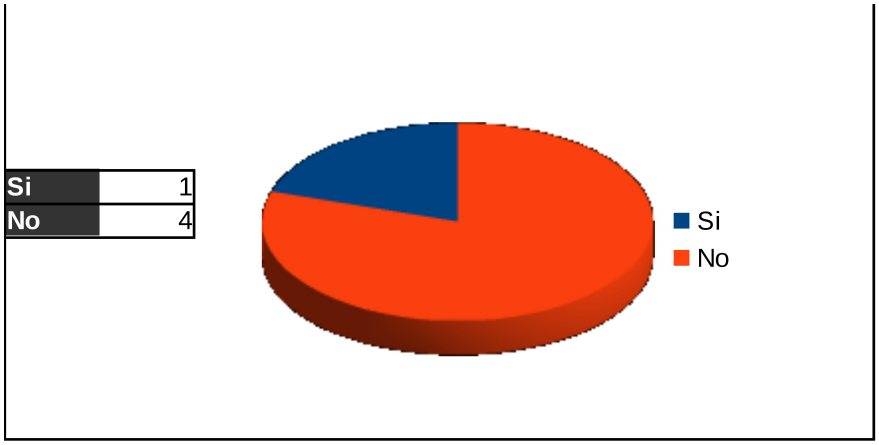

Figura 48: Respuesta item 18 Definición

Fuente: Elaboración propia.

19)¿Se busca crear conductas que favorezcan los valores éticos, con respecto al manejo de la información?

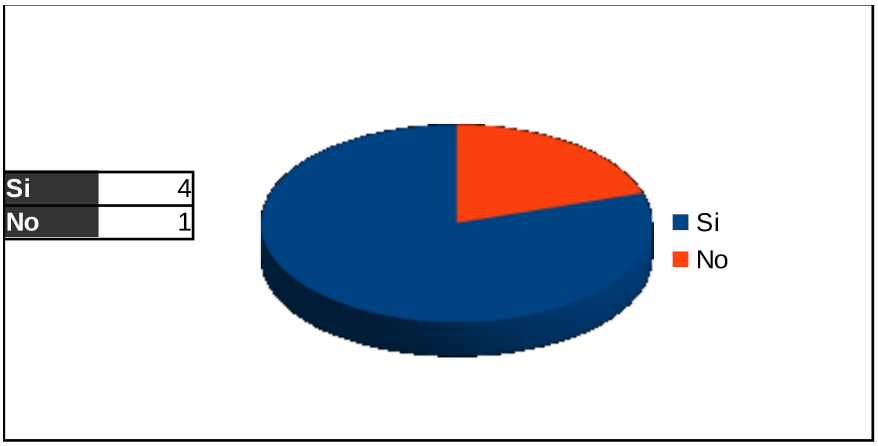

Figura 49: Respuesta item 19 Definición

Fuente: Elaboración propia.

20)¿Se promueve la implementación de medidas que contribuyan a mejorar la seguridad?

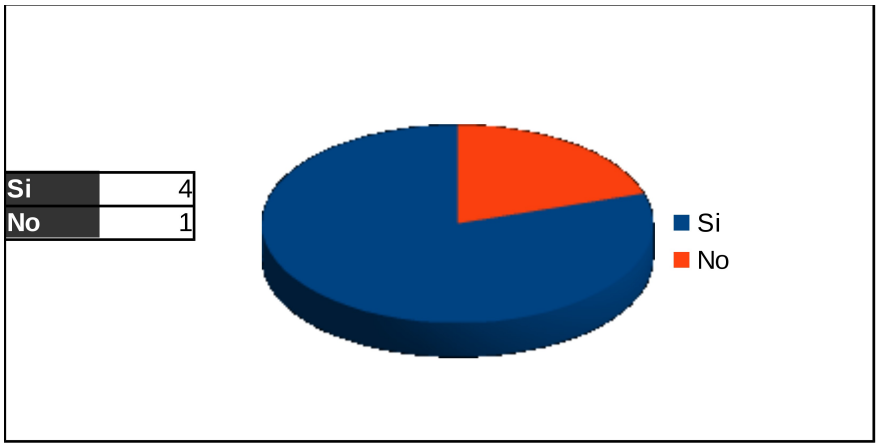

Figura 50: Respuesta item 20 Definición

Fuente: Elaboración propia.

21)¿Se establecen medidas que induzcan al personal a acatar la normativa existente en materia de la seguridad de la información?

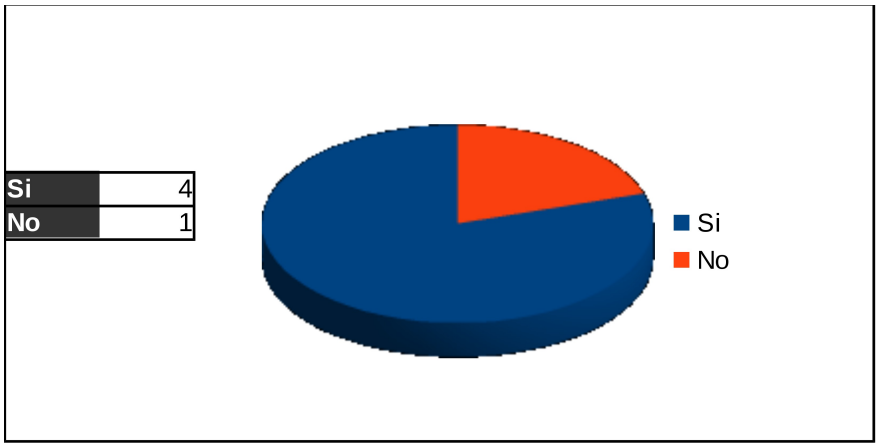

Figura 51: Respuesta item 21 Definición

Fuente: Elaboración propia.

22)¿Están claramente definidos los roles que en materia de la seguridad de la información juegan cada uno de los involucrados en el manejo de la información institucional?

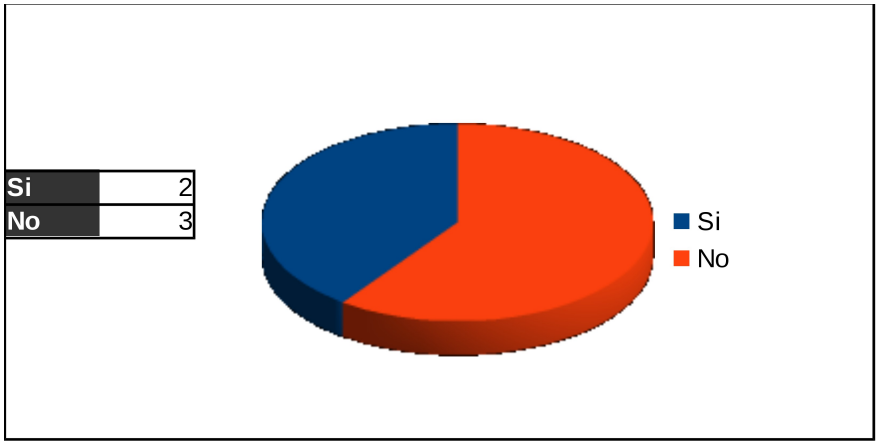

Figura 52: Respuesta item 22 Definición

Fuente: Elaboración propia.

23)¿Hay estrategias tendientes a mejorar las falencias en materia de seguridad de la información que permitan trazar un camino a seguir en esta materia?

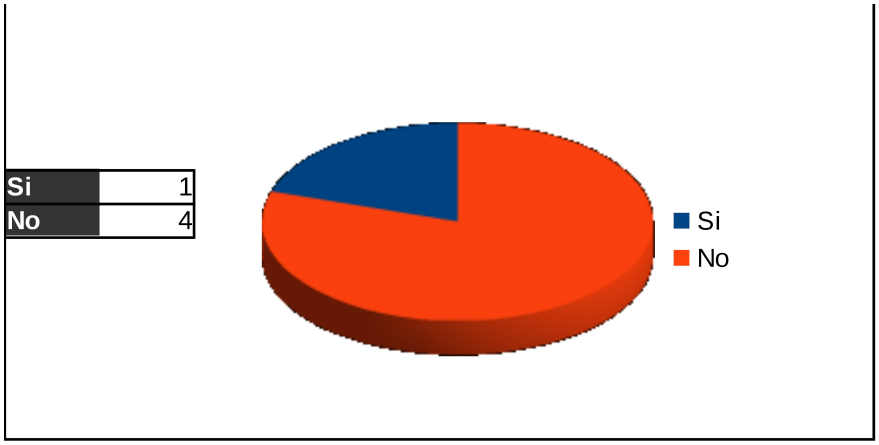

Figura 53: Respuesta item 23 Definición

Fuente: Elaboración propia.

Nivel Gestión

1)¿Se promueve en la institución el aprendizaje en conjunto de los miembros del equipo de trabajo?

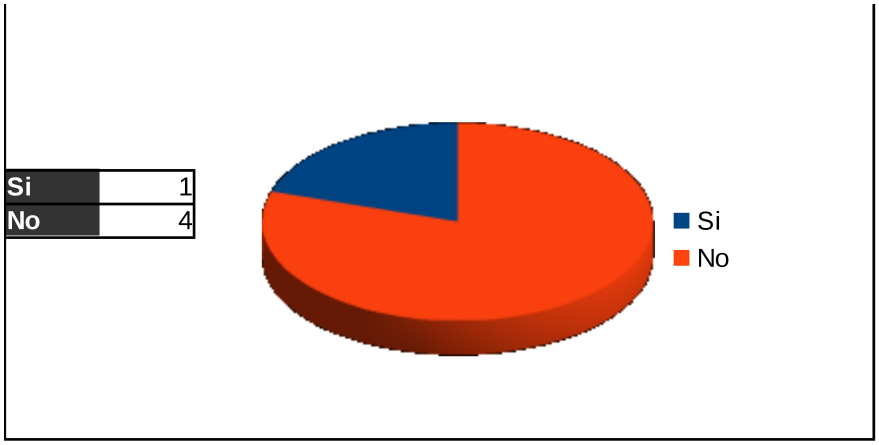

Figura 54: Respuesta item 1 Gestión

Fuente: Elaboración propia.

2)¿Existe una visión compartida entre los miembros de la Unidad a cargo de la Seguridad de la Información

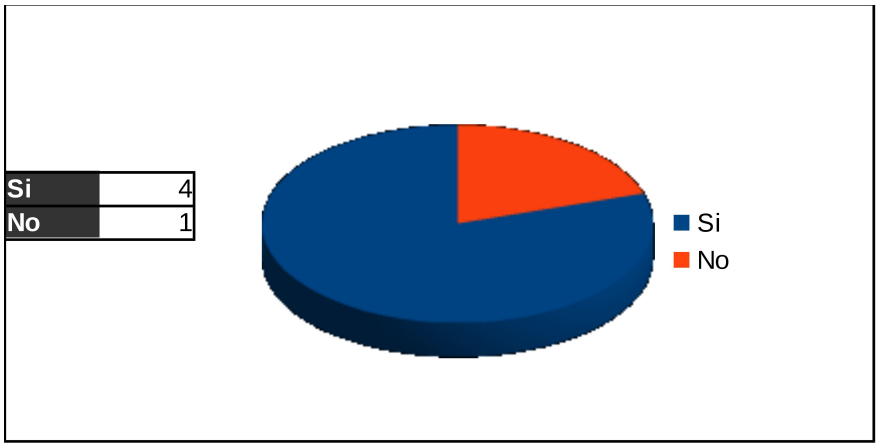

Figura 55: Respuesta item 2 Gestión

Fuente: Elaboración propia.

3)¿Se considera que todos los personales con rango directivo son actores principales en el objetivo de garantizar la seguridad de la información?

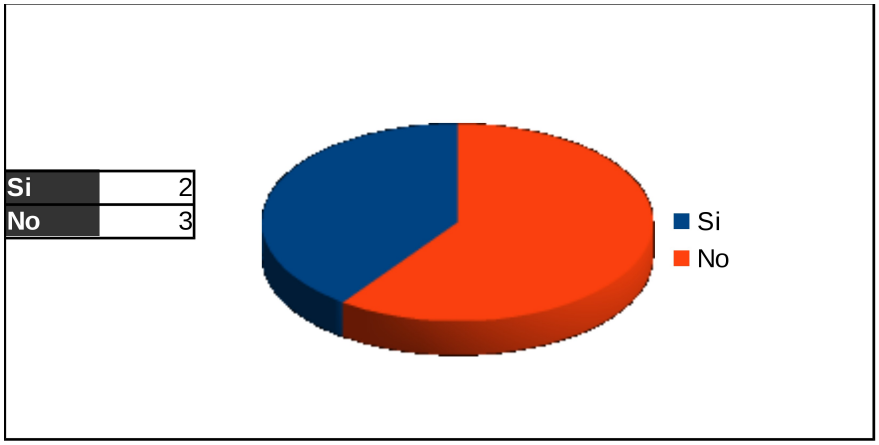

Figura 56: Respuesta item 3 Gestión

Fuente: Elaboración propia.

4)¿Se realiza auditoría interna sobre la Seguridad de la Información?

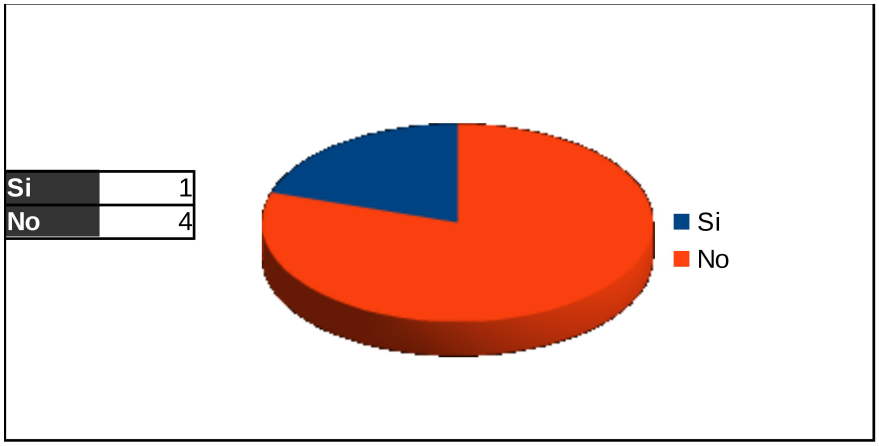

Figura 57: Respuesta item 4 Gestión

Fuente: Elaboración propia.

5)¿Se realiza auditoría externa sobre la Seguridad de la Información?

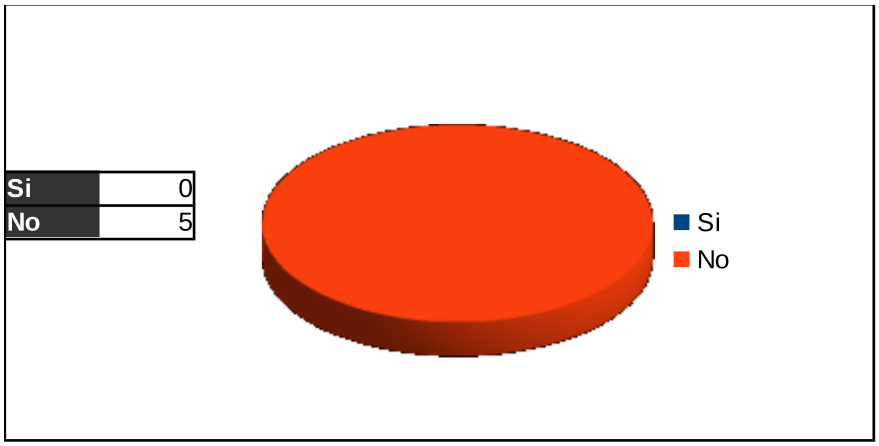

Figura 58: Respuesta item 5 Gestión

Fuente: Elaboración propia.

6)¿Existe un plan estratégico para garantizar la Seguridad de la Información en la Institución?

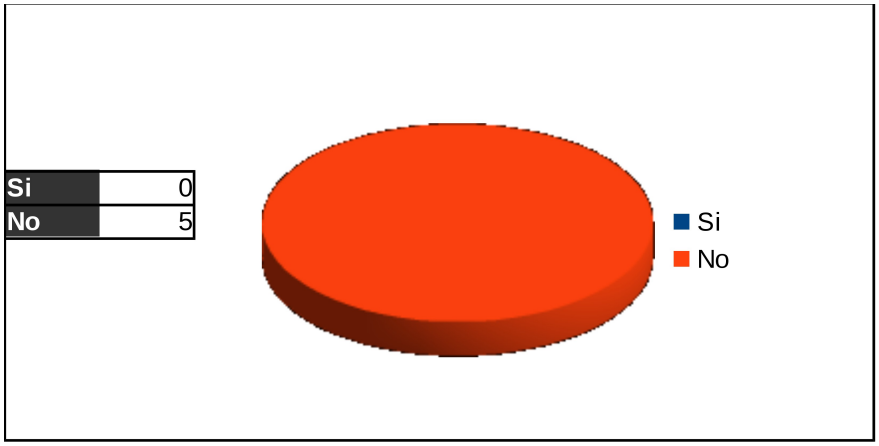

Figura 59: Respuesta item 6 Gestión

Fuente: Elaboración propia.

7)¿Se manejan niveles de autorización para que los usuarios puedan acceder a los datos y recursos en el ejercicio diario de sus funciones?

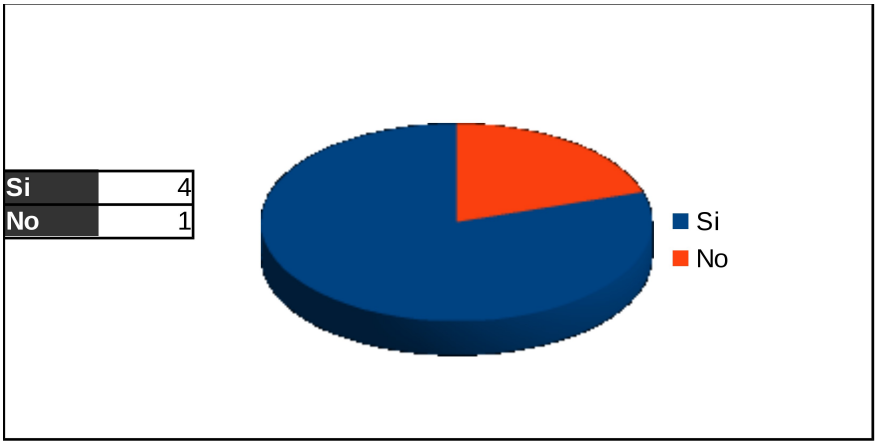

Figura 60: Respuesta item 7 Gestión

Fuente: Elaboración propia.

8)¿Se lleva un control de acceso físico para determinados sitios de la institución, de acuerdo a las funciones del empleado?

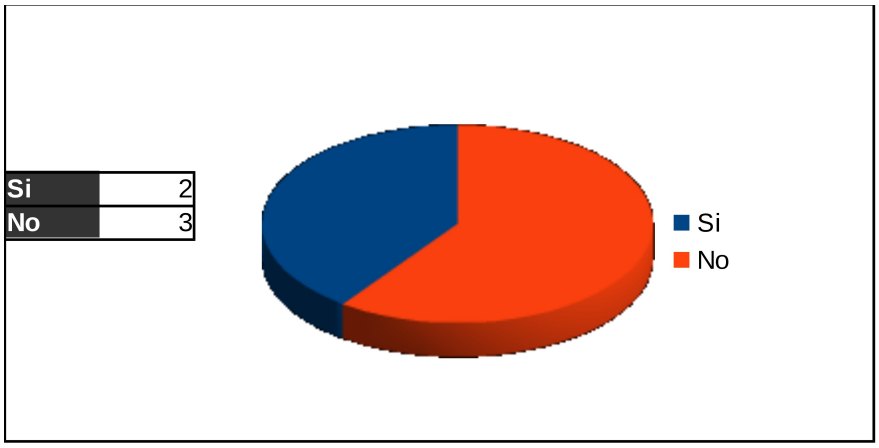

Figura 61: Respuesta item 8 Gestión

Fuente: Elaboración propia.

9)¿Es efectiva la gestión del soporte en el área de Seguridad de la Información?

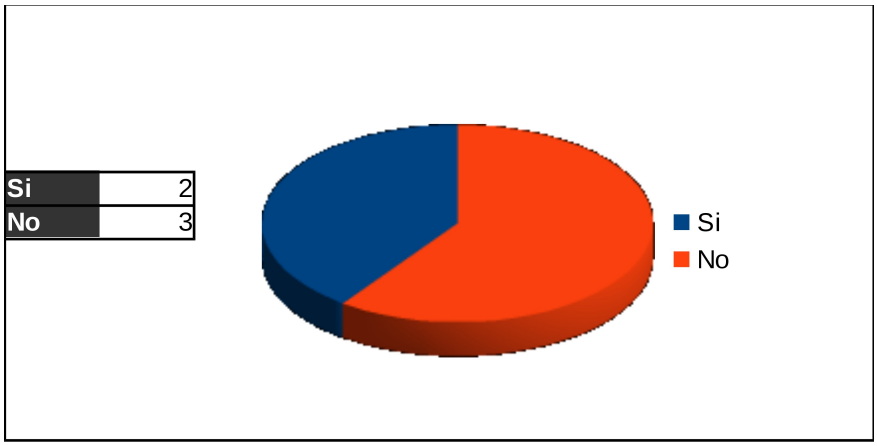

Figura 62: Respuesta item 9 Gestión

Fuente: Elaboración propia.

10)¿Se cumple la Política de Confidencialidad de la Información?

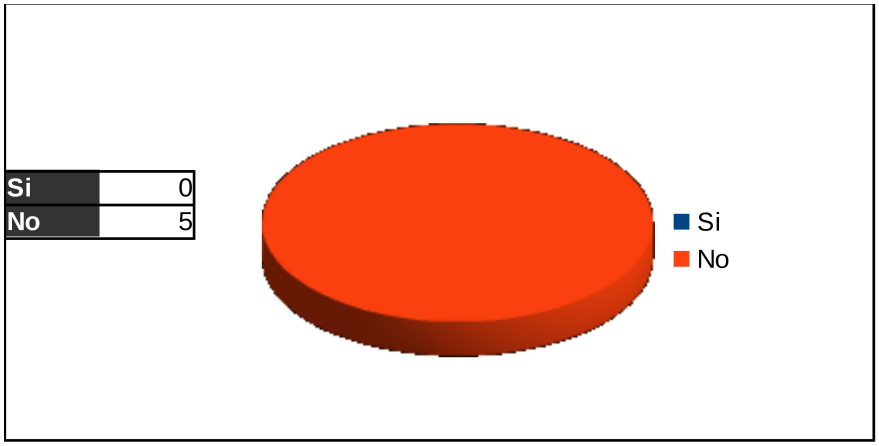

Figura 63: Respuesta item 10 Gestión

Fuente: Elaboración propia.

11)¿Se cumple la Política de Integridad de la Información?

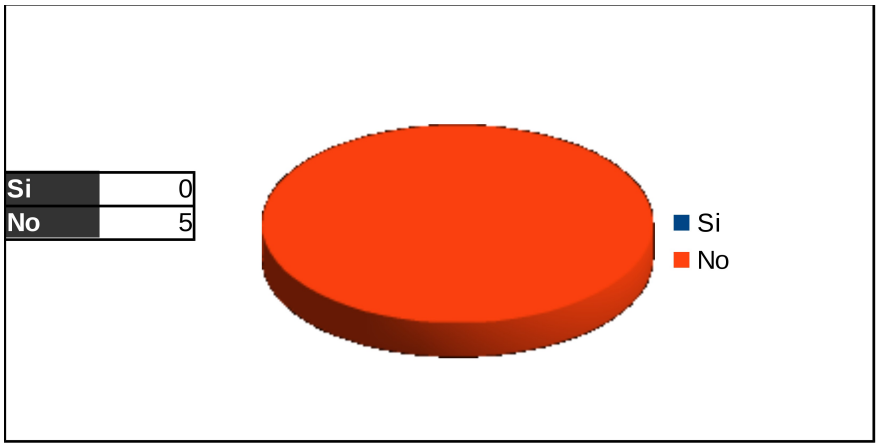

Figura 64: Respuesta item 11 Gestión

Fuente: Elaboración propia.

12)¿Se cumple la Política de la Disponibilidad de la Información?

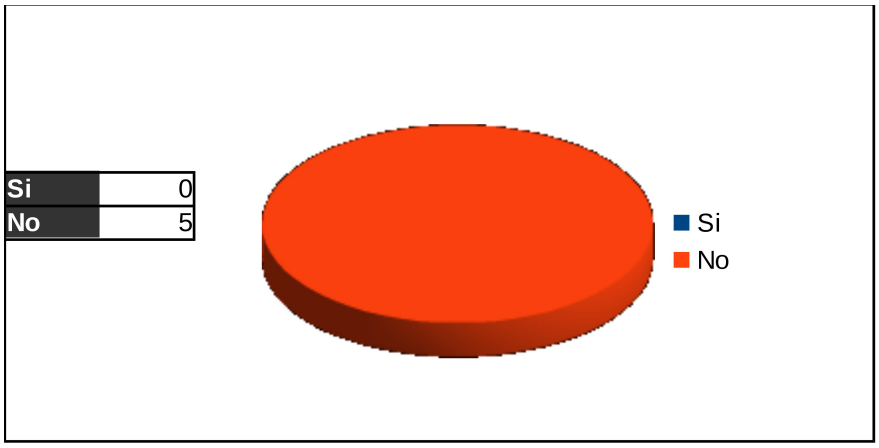

Figura 65: Respuesta item 12 Gestión

Fuente: Elaboración propia.

13)¿Se cumple la Política en materia de Autenticidad de la Información?

Figura 66: Respuesta item 13 Gestión

Fuente: Elaboración propia.

14)¿Se cumple la Política en materia de Autorización de acceso a los datos?

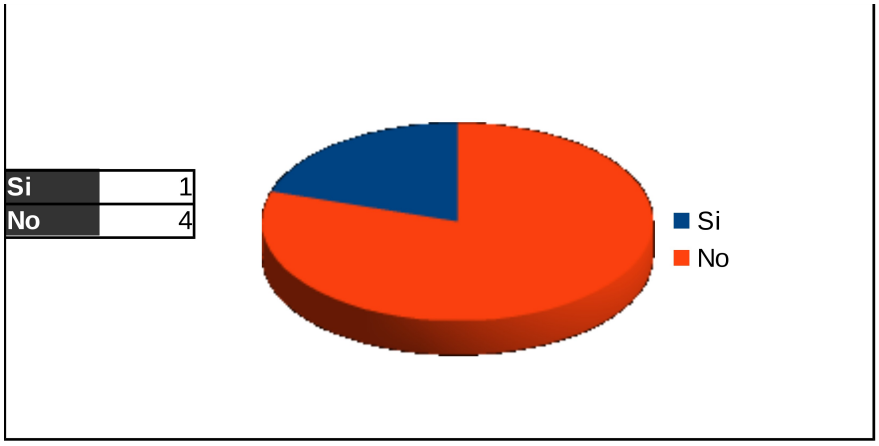

Figura 67: Respuesta item 14 Gestión

Fuente: Elaboración propia.

15)¿Se cumple la Política de Firmas Electrónicas?

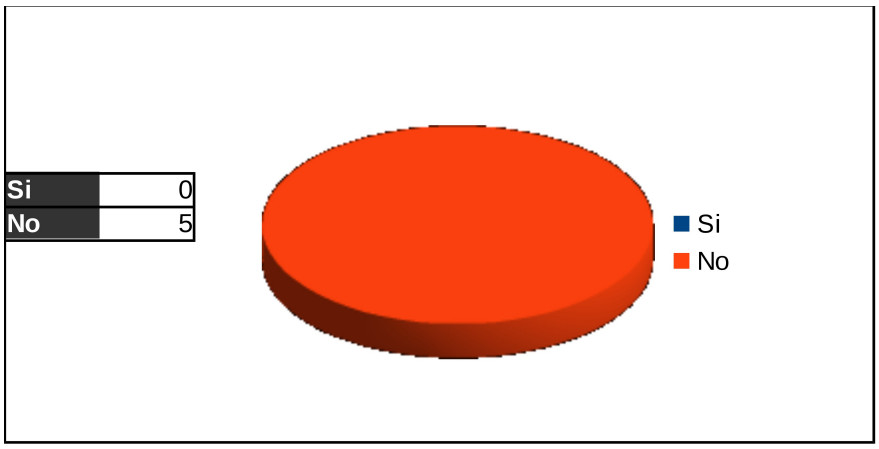

Figura 68: Respuesta item 15 Gestión

Fuente: Elaboración propia.

16)¿Se cumple la Política de Certificados Digitales?

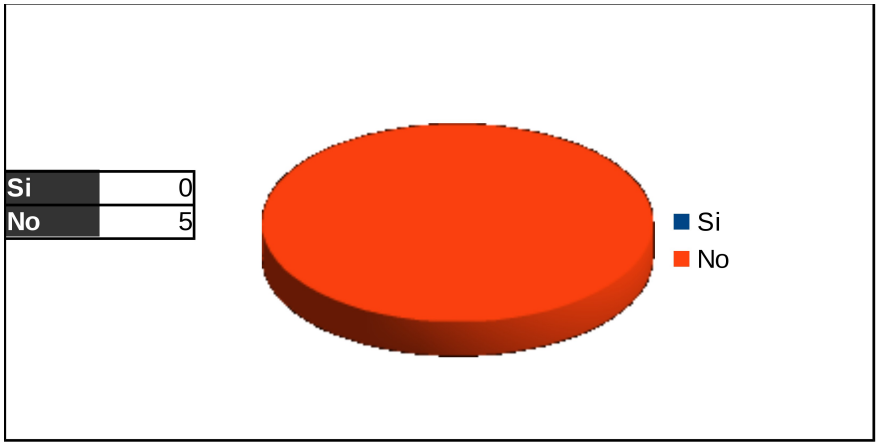

Figura 69: Respuesta item 16 Gestión

Fuente: Elaboración propia.

17)¿Se identifica el personal de la institución con los valores éticos de la Seguridad de la Información?

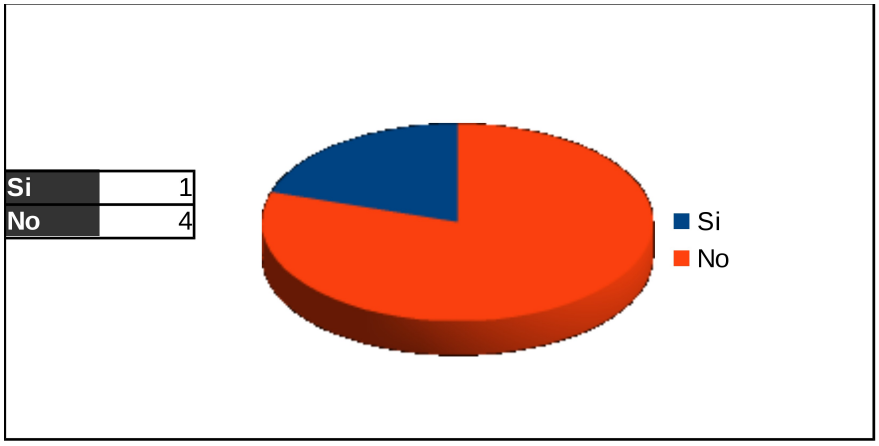

Figura 70: Respuesta item 17 Gestión

Fuente: Elaboración propia.

18)Se establecen planes para la mejora contínua de los niveles de Seguridad de la Información?

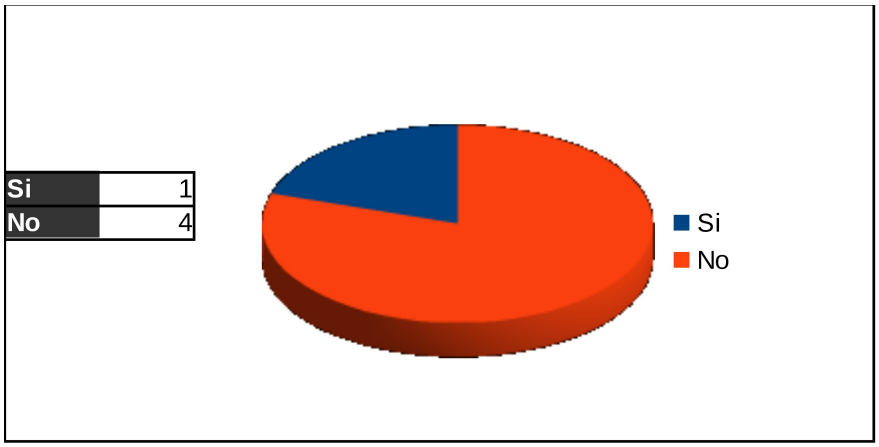

Figura 71: Respuesta item 18 Gestión

Fuente: Elaboración propia.

19) Se discute al mas alto nivel el estado de la Seguridad de la Información?

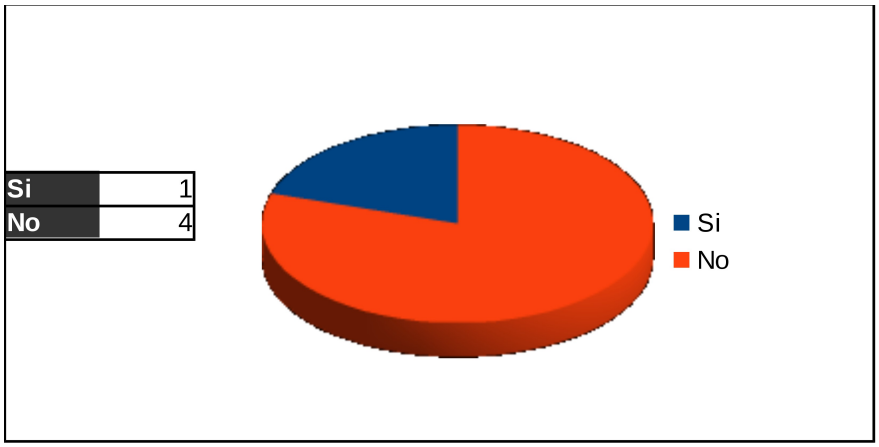

Figura 72: Respuesta item 19 Gestión

Fuente: Elaboración propia.

Nivel Óptimo

1)¿Los cambios o implementaciones en Seguridad de la Información se realizan en equipo y de manera planificada?

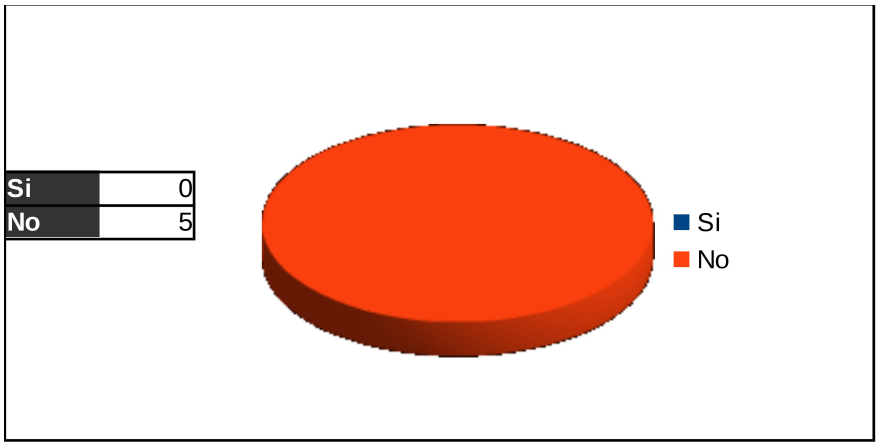

Figura 73: Respuesta item 1 Óptimo

Fuente: Elaboración propia.

2)¿Se realizan actualizaciones y difusión permanente de las Políticas de Seguridad de la Información?

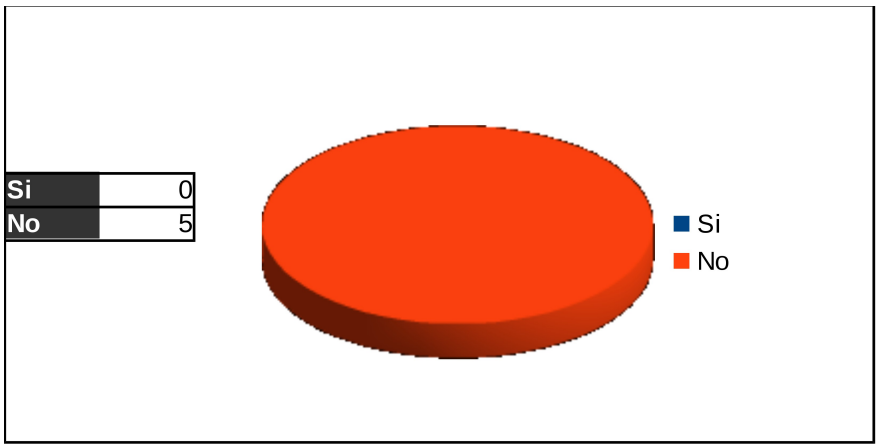

Figura 74: Respuesta item 2 Óptimo

Fuente: Elaboración propia.

3)¿Aplica el conjunto de los empleados de la Institución las Políticas de Seguridad de la Información?

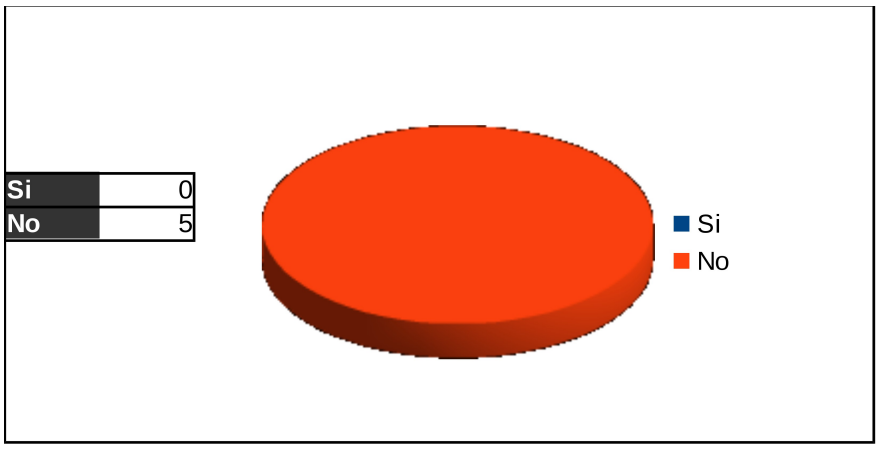

Figura 75: Respuesta item 3 Óptimo

Fuente: Elaboración propia.

4)¿Existe un criterio uniforme en cuanto a la aplicación de medidas que ayuden a fomentar la Seguridad de la Información?

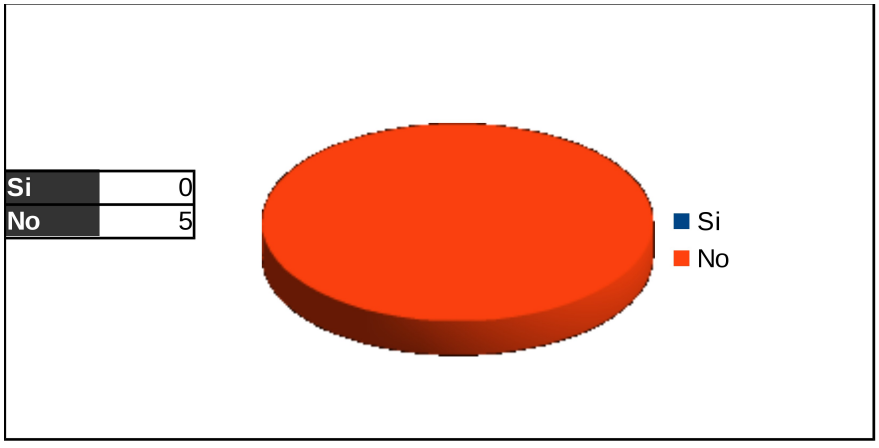

Figura 76: Respuesta item 4 Óptimo

Fuente: Elaboración propia.

5)¿Existe cultura organizacional en materia de la Seguridad de la Información que se pueda considerar uniforme?

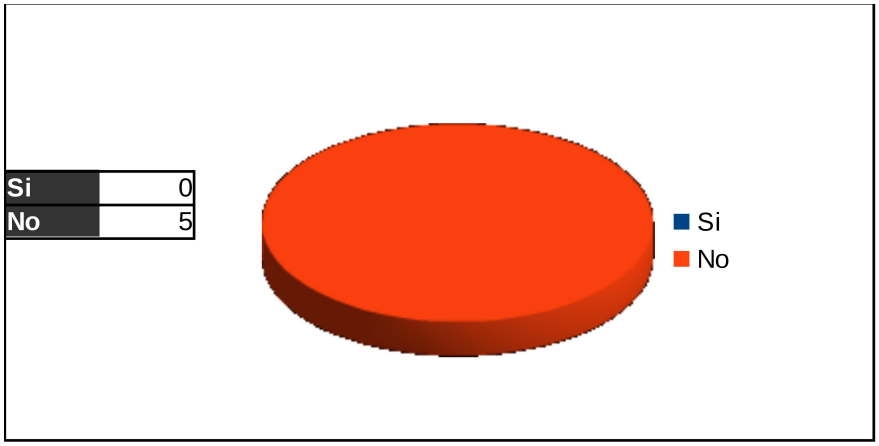

Figura 77: Respuesta item 5 Óptimo

Fuente: Elaboración propia.

6)¿Existe alineación entre las medidas institucionales de salvaguarda con las especificadas en el plan estratégico de Seguridad de la Información?

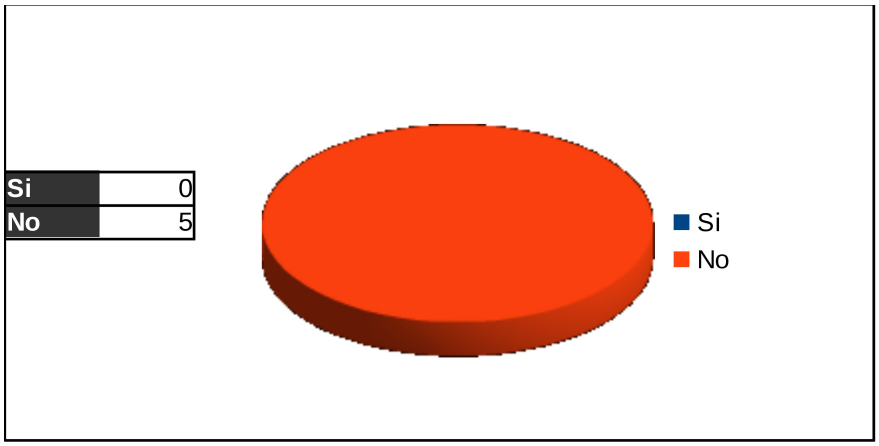

Figura 78: Respuesta item 6 Óptimo

Fuente: Elaboración propia.

7)¿Considera que a todo nivel en la Institución los equipos de trabajo que se conforman comparten la visión en Seguridad de la Información?

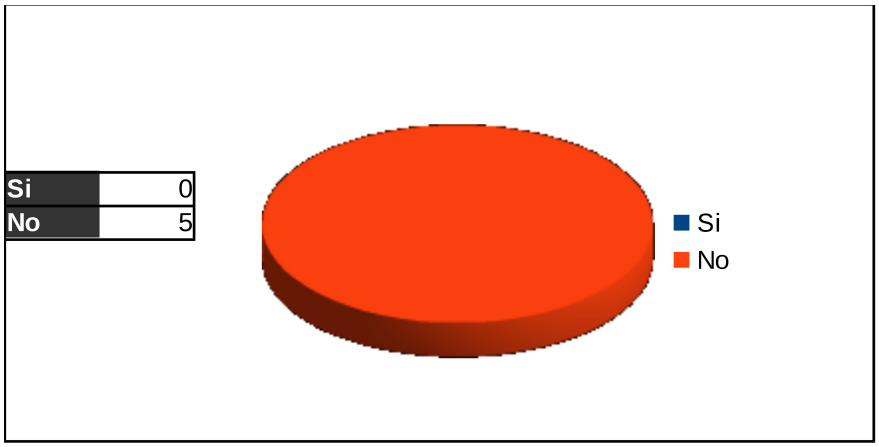

Figura 79: Respuesta item 7 Óptimo

Fuente: Elaboración propia.

8)¿Forman parte de la cultura institucional los valores éticos de la Seguridad de la Información?

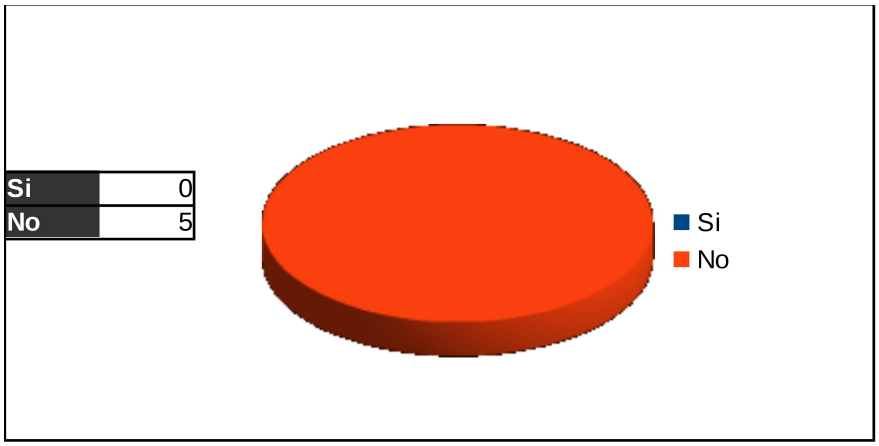

Figura 80: Respuesta item 8 Óptimo

Fuente: Elaboración propia.

9)¿Hay actualización del nivel de formación en materia de Seguridad de la Información en el equipo de trabajo del área informática?

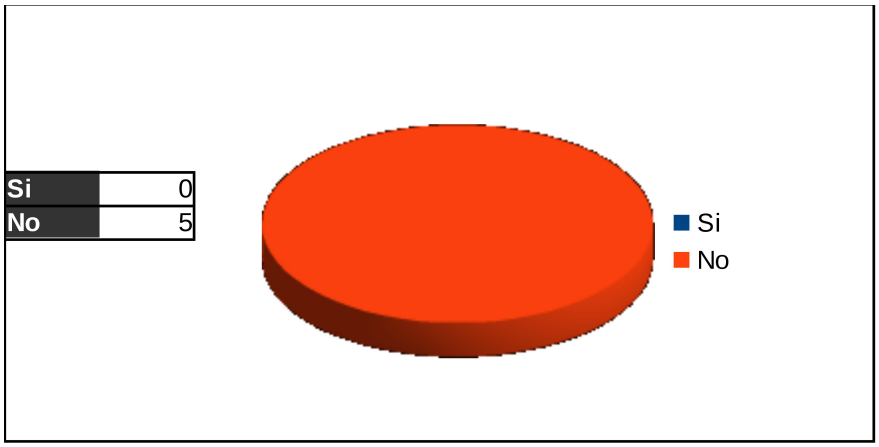

Figura 81: Respuesta item 9 Óptimo

Fuente: Elaboración propia.

10)¿Hay proactividad en las actuaciones del equipo a cargo de la Seguridad de la Información en la Institución?

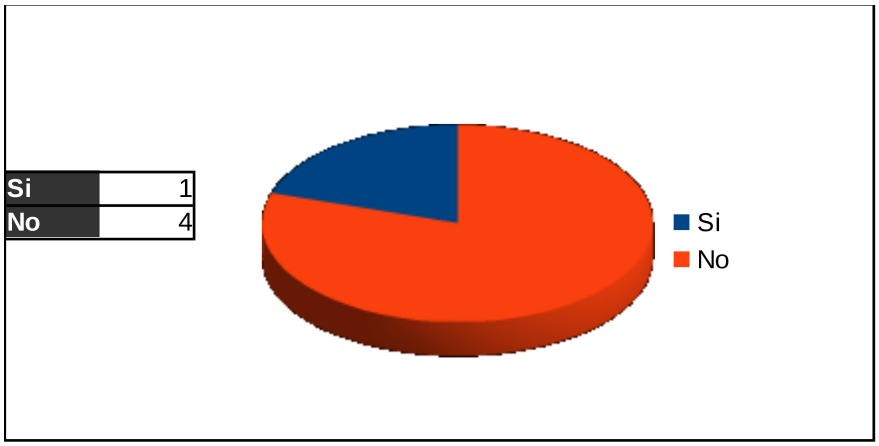

Figura 82: Respuesta item 10 Óptimo

Fuente: Elaboración propia.

11)¿Se Aplican con frecuencia Metodologías de Análisis y Control de Riesgo?

Figura 83: Respuesta item 11 Óptimo

Fuente: Elaboración propia.

12)¿Existe un registro de activos informáticos (Software y Hardware) de la Institución?

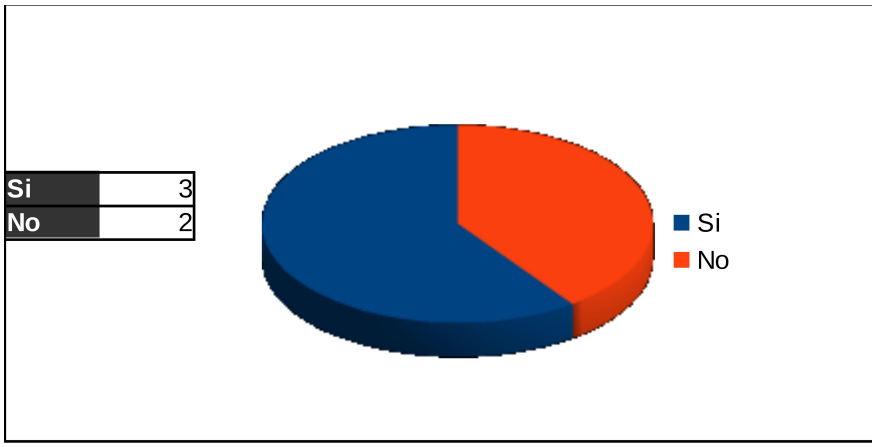

Figura 84: Respuesta item 12 Óptimo

Fuente: Elaboración propia.

13)¿Existen niveles de comunicación entre los equipos de cada una de las áreas informáticas de la institución y el equipo a cargo de la Seguridad de la Información?

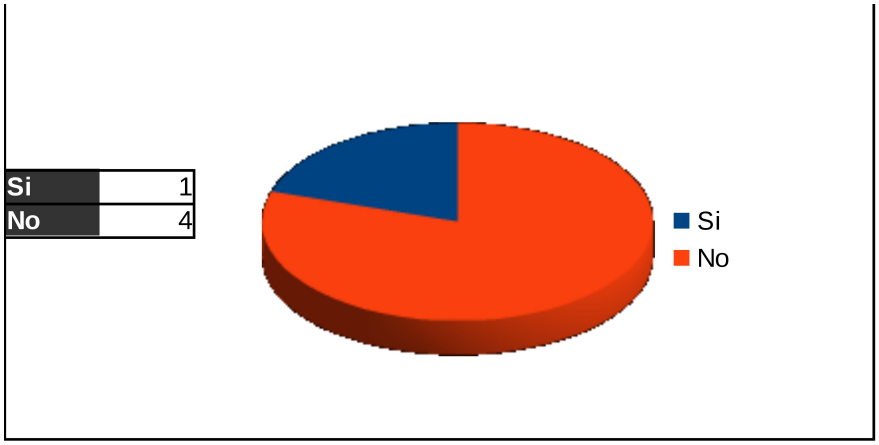

Figura 85: Respuesta item 13 Óptimo

Fuente: Elaboración propia.

14)¿Se desarrollan en conjunto los planes estratégicos, con la programación de la Seguridad de la Información?

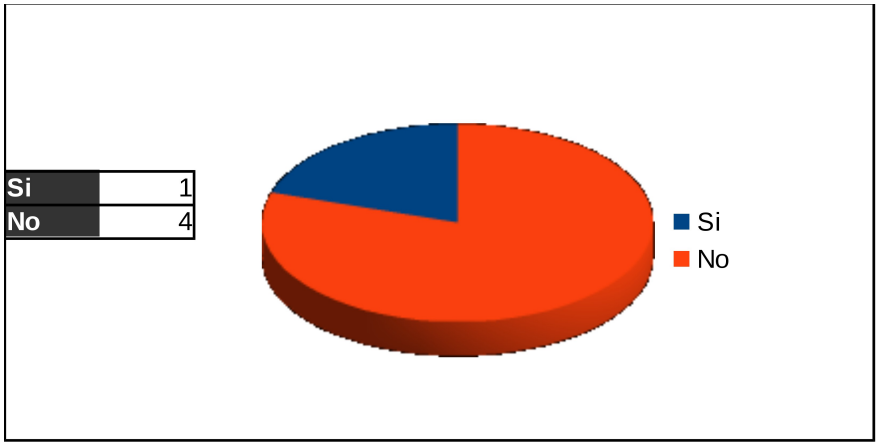

Figura 86: Respuesta item 14 Óptimo

Fuente: Elaboración propia.

15)¿Se realiza un análisis y gestión de riesgo de los nuevos activos incorporados a la institución?

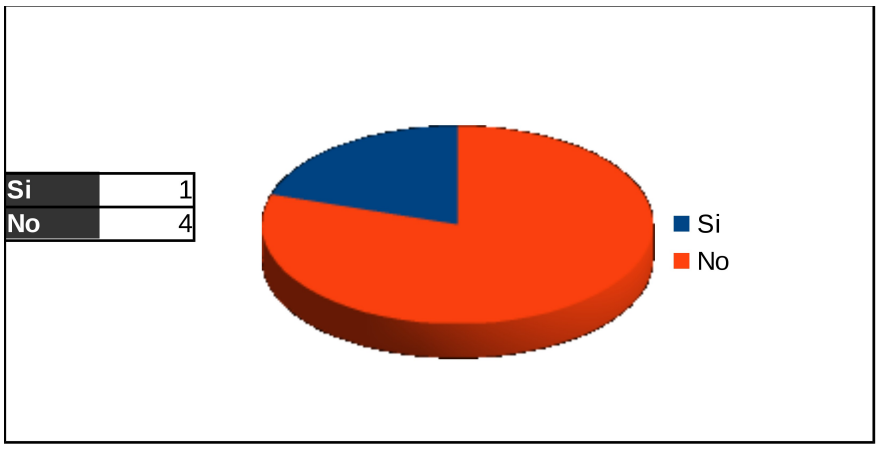

Figura 87: Respuesta item 15 Óptimo

Fuente: Elaboración propia.

16)¿Se aplican y desarrollan políticas propias en materia de la Seguridad de la Información?

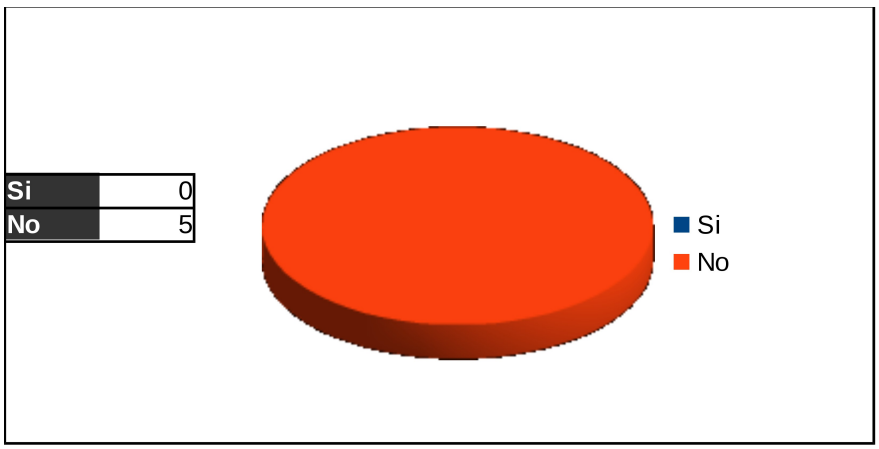

Figura 88: Respuesta item 16 Óptimo

Fuente: Elaboración propia.

17)¿Se cumplen a todos los niveles con las Políticas que le corresponde a cada uno de los usuarios de acuerdo a la naturaleza de sus funciones?

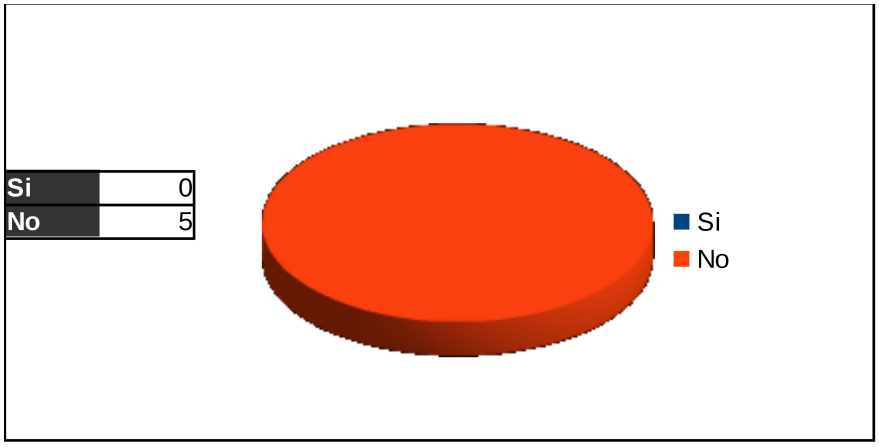

Figura 89: Respuesta item 17 Óptimo

Fuente: Elaboración propia.

18)¿Esta involucrada toda la Institución en la Seguridad de la Información?

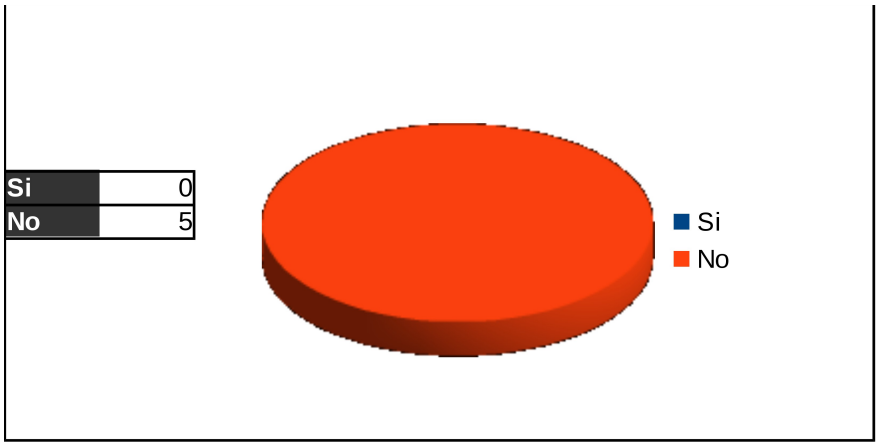

Figura 90: Respuesta item 18 Óptimo

Fuente: Elaboración propia.

19)¿Se elaboran campañas destinadas a masificar el conocimiento de las nuevas Políticas de Seguridad de la Información?

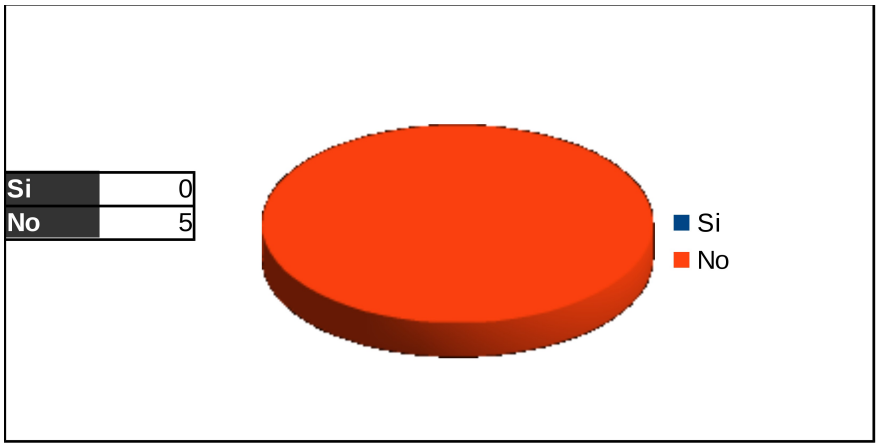

Figura 91: Respuesta item 19 Óptimo

Fuente: Elaboración propia.

ANEXO D

Resultados del cuestionario para la elaboración del Modelo de Madurez

Instrucciones: Lea las siguientes interrogantes y conteste de acuerdo a la frecuencia con la que ocurre el evento, tomando en consideración los siguientes valores:

5 Siempre 4 Casi siempre 3 Algunas veces 2 Casi nunca 1 Nunca

	NIVEL DE INICIO	5	4	3	2	1
1	¿Se realizan chequeos de Seguridad de la Información de Manera periódica?			3	2	
2	¿Los incidentes asociados a la Seguridad de la Información conducen a impacto de consideración con que frecuencia?			3	2	

	NIVEL DE RECONOCIMIENTO	5	4	3	2	1
1	¿Se revisa de manera cotidiana el tema de la Seguridad de la Información, en las diversas áreas?			3	1	1
2	¿Con que frecuencia el impacto de los incidentes de seguridad tienen consecuencias de máximo impacto?				4	1
3	¿Con que frecuencia se definen las responsabilidades en materia de seguridad de la información				5	
4	¿Con que frecuencia se pierden los esfuerzos en materia de seguridad de la información, que son implementados en la plataforma institucional?			2	3	

	NIVEL DE DEFINICIÓN	5	4	3	2	1
1	¿La plataforma tecnológica de la institución se		3	2		

	actualiza de manera periódica?					
2	¿La plataforma cuenta con soluciones antivirus, antiespias, anti SPAM y otros anti Malware, que en caso de ser licenciados son actualizados una vez que llega al termino la duración de las licencias?		5			
3	¿Se realiza un monitoreo para evaluar el comportamiento de la red de manera cotidiana?			2	3	
4	¿Se llevan estadísticas y bitácoras que registren el comportamiento de la red?				5	
5	¿Se realizan respaldos de todos los activos críticos de la plataforma?			2	3	
6	¿Se debe contar con autorización para el acceso a los aplicativos, equipos y demás recursos para que los usuarios cumplan con sus funciones?	5				
7	¿El acceso físico a las áreas críticas de la institución es registrado regularmente?					5

	NIVEL DE GESTIÓN	5	4	3	2	1
1	¿La institución tiene un registro detallado de los incidentes de seguridad?		1	3	1	
2	¿Tiene la institución registro automatizado de los eventos que puedan comprometer la seguridad informática de la plataforma?				4	1
3	¿Hay difusión masiva de los planes en materia de seguridad informática?					5
4	¿El trabajo en materia de seguridad informática se maneja al mas alto nivel en la institución?			1	3	1
5	¿Están definidos los valores éticos de la Seguridad de la Información?		2	3		
6	¿Hay difusión masiva de los valores éticos de la Seguridad de la Información?				4	1
7	¿Se ofrecen al personal directivo charlas, cursos, seminarios, con la finalidad de crear cultura organizacional en materia de seguridad de la información?					5
8	Se ofrecen al personal no directivo charlas,					5

	cursos, seminarios, con la finalidad de crear cultura organizacional en materia de seguridad de la información?					
9	¿Se ofrecen al personal técnico en el área de informática charlas, cursos, seminario, con la finalidad de crear cultura organizacional en materia de seguridad de la información?					5
10	¿En las reuniones entre los distintos departamentos se fomenta la creación de cultura organizacional, en materia de Seguridad de la Información?				4	1
11	¿Se fomenta la formación de hábitos que promuevan los valores éticos, con respecto al manejo de la información?			3	2	
12	¿Se maneja a todo nivel los servicios de confidencialidad, integridad, autenticidad, autorización y disponibilidad de la información?			2	3	
13	¿Se tiene un control del valor de los activos de la institución?		1	3	1	
14	¿Se mantiene actualizado el valor de los activos institucionales?			3	2	

	NIVEL ÓPTIMO	5	4	3	2	1
1	¿La toma de decisiones en materia de seguridad de la información cuenta con el apoyo de las máximas autoridades de la institución?		4	1		
2	¿La gestión de la seguridad de la información lleva un control de eventos?			3	2	
3	¿La difusión de las Políticas de Información se realiza a todos los niveles del personal?				4	1
4	¿El Soporte del área de a Seguridad Informática es medido para conocer la efectividad de dicha tarea?					5
5	¿Se toman decisiones en el área de la Seguridad Informática en función de los registros de incidentes y demás eventos en el área?					5
6	¿Se toman decisiones al más alto nivel en		1	3	1	

	función de la gestión de los servicios de confidencialidad, integridad, autenticidad, autorización y disponibilidad de la información?					
7	¿El personal de la institución esta identificado con los valores de Seguridad de la Información?		1	2	2	
8	¿Se mantienen actualizadas las Políticas de Seguridad de la Información en la Institución?				2	3
9	¿Hay Metodología de Seguridad de la Información que dicte los patrones a seguir en la materia?				4	1

Muy agradecido por la colaboración prestada en el desarrollo del presente trabajo de investigación.

Anexo E

Entrevista para sondear los niveles de seguridad de la información en Instituciones Públicas

El objetivo del presente instrumento es conocer el estado actual de la Seguridad Informática en la Plataforma institucional para la que usted trabaja, esto enmarcado dentro de un trabajo de investigación orientado a determinar ese estado en la Administración Pública Nacional de Venezuela.

La investigación procura medir el estado de madurez del Monitoreo de Seguridad Informática para tomar las correspondientes medidas y por ende incrementar los niveles de seguridad en la mencionada plataforma.

Conteste de la manera mas precisa posible a las siguientes interrogantes

1.- ¿Cual cree usted que es la mayor el mayor obstáculo que presenta la institución en materia de la seguridad de la información?

2.- ¿La institución que representa posee una estructura encargada de gestionar los procesos de la Seguridad de la Información?

3.- ¿Se realiza mantenimiento periódico a los sistemas y servicios informáticos de la institución, procurando minimizar las brechas de seguridad que suelen abrirse como consecuencia de errores en el diseño de aplicativos y sistemas en general?

4.- ¿En materia de respaldo de la información, considera usted que la institución que representa tiene un esquema que permita realizar de una manera adecuada , la recuperación de datos eventualmente afectados por un incidente?

5.- ¿Se tienen definidas políticas para la realización de copias de seguridad de los datos?

6.- ¿Los programas que se utilizan en la institución que representa, que almacenan datos, cumplen con las características de seguridad descritas en las políticas de seguridad de la información redactadas con ese fin?

7.- ¿Cuál cree usted sería el mecanismo más eficiente para realizar el seguimiento de los equipos que conforman el parque tecnológico de la institución?

8.- ¿En materia de monitoreo de seguridad de la información, considera usted que los eventos que ocurren en la plataforma son correlacionados de manera adecuada?

9.- ¿Qué tipo de mecanismos usted recomendaría para poder realizar un análisis de los eventos asociados a incidentes de seguridad, que permitan tener un control de dichos eventos y adicionalmente tomar decisiones en función de minimizarlos?

10.- ¿Cómo recomendaría usted poder validar y evaluar el rubro de la seguridad informática en la plataforma institucional?

11.- ¿Cuáles controles para la mitigación de riesgos usted propondría para implantar en la institución que representa?

12.- ¿Con qué frecuencia cree usted debería reunirse la dirección del área informática, con las máximas autoridades de la institución, para discutir las necesidades de la seguridad de la información en el ente para el que trabaja?

13.- ¿Se ha tenido en cuenta la seguridad informática como criterio en las fases de desarrollo y puesta en producción de las aplicaciones usadas en los proyectos de la institución?

14.- ¿Se han establecido controles adecuados para garantizar la disponibilidad, confidencialidad e integridad de los datos manejados por su institución?

15.- ¿Se tiene definida una política de restauración y recuperación de los sistemas en caso de eventos que pudieran derivar en perdida de datos sensibles?

16.- En materia de Gestión de la Seguridad de la Información, ¿se cuenta con un presupuesto y cual suele ser el uso que se le da a dichos fondos?

17.- ¿Los eventos de seguridad de la información considera usted que al momento de ocurrir tienen un tratamiento adecuado y que recomendaciones básicas podría dar en caso de considerar que no lo tienen?

18.- ¿Cada cuanto tiempo son evaluados los mecanismos de seguridad de la información con que cuenta la Institución para minimizar las brechas de seguridad que pudieran presentarse en la plataforma tecnológica?

19.- ¿Hay una alineación entre las políticas de seguridad de la información y la misión, visión y lineas estratégicas de la Institución que usted representa?

20.- ¿Como considera usted que pueden implementarse mecanismos que coadyuven a mejorar los niveles de seguridad de la información actualmente presentes en su institución?

Muy agradecido por la colaboración prestada en el desarrollo del presente trabajo de investigación.