UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA
ESPECIALIZACIÓN EN COMUNICACIONES Y REDES DE COMUNICACIÓN DE DATOS

"DISEÑO DE UNA METODOLOGÍA E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA RED DE COMUNICACIONES DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN SUPERIOR"

Autor: Ing. Erika A. Olivares P.

Caracas, Mayo 2008

TRABAJO ESPECIAL DE GRADO

"DISEÑO DE UNA METODOLOGÍA E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA RED DE COMUNICACIONES DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN SUPERIOR"

TUTOR Académico: Prof.: Vincenzo Mendillo

Presentado ante la ilustre
Universidad Central de
Venezuela para optar al Título
De Especialista en Comunicaciones y Redes de Comunicación de Datos
Por la Ing. Erika A. Olivares Penso .

CARACAS, MAYO 2.008

DEDICATORIA

A todas aquellas persona que me ayudaron y
me dieron la fuerza para seguir adelante,
creyeron en mí, y siempre me dieron su apoyo
en especial a mis padres Jesús y Auristela,
y mis hermanos, a los que espero éste sea un ejemplo
lleno de constancia y perseverancia,
A mi Esposo Guilmen y a mi Tía Isora por su interés
contínuo en que culminara este proyecto.
A ti María Francia, querida amiga,
por tu ayuda, y por tu consecuente apoyo
y a todas esas personas
que aunque no estén físicamente
están siempre cerca, para llenarnos de
muchas satisfacciones espirituales.

AGRADECIMIENTOS

Ante todo le doy gracias a Dios, que siempre me ha guiado por los mejores caminos, siempre me ha protegido y me ha dado fuerzas y esperanzas cuando lo he necesitado.

A todos mis seres queridos, a mis padres Jesús y Auristela, quienes siempre han estado en los momentos mas importantes de mi vida. A mi esposo Guilmen por su comprensión, amor, y apoyo en todo lo que hago. A mis abuelos Albina y Alonso quienes siguen a mi lado brindándome todo su cariño, a mis abuelos paternos Atilano y Sila quienes ya no están en este mundo pero se que siempre están a mi lado, a mis tías y demás familiares y a todos esas personas especiales que están muy cerca de mí en las buenas y en las malas.

Le agradezco sinceramente al Profesor Luis Augusto Acuña Cedeño, Ministro del Poder Popular para la Educación Superior, por su apoyo y colaboración para llevar a cabo este trabajo.

Un agradecimiento muy especial al profesor Vincenzo Mendillo por la confianza, la paciencia, la tolerancia y por sobre todas las cosas, por enseñarme a que simplemente uno debe hacer lo que se propone y de la mejor forma para que todo tenga siempre una razón de ser. Quiero agradecer además muy cariñosamente a la Sra. Gipsy de Postgrado, por toda su colaboración y apoyo entoda la especialización.

También le agradezco enormemente a todas las personas que colaboraron conmigo en éste proyecto, como personal del Ministerio del Poder Popular para la Educación Superior, y a mis compañeros y amigos del Postgrado, simplemente por atenderme, enseñarme y darme la oportunidad de compartir con ellos, que Dios los bendiga.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

"DISEÑO DE UNA METODOLOGÍA E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA RED DE COMUNICACIONES DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN SUPERIOR"

Autor: Ing. Erika Alejandra Olivares Penso
Tutor: Prof. Vincenzo Mendillo
Mayo 2008

RESUMEN

El objetivo principal de este trabajo es diseñar una metodología e implementar políticas de seguridad en la red de comunicaciones del Ministerio del Poder Popular para la Educación Superior

Para lograr este objetivo se realizaron diferentes actividades. Se llevó a cabo un estudio de la situación actual para conocer el estado de los activos de la institución, así como el manejo de la información dentro de la misma, para luego establecer las necesidades en cuanto a la seguridad requerida para el resguardo de dichos activos**.** En el levantamiento de información también se consideraron las bases teóricas sobre los aspectos concernientes a la seguridad de información y todas aquellas actividades necesarias para poder establecer políticas sobre las mismas, tal como es el caso de un análisis de riesgos de activos de información. Con lo anterior se obtuvo la base para proceder con la propuesta de dichas políticas de seguridad.

El diseño efectuado en este trabajo sentará las bases para su implementación y revisión contínua usando herramientas como análisis de riesgo para la toma de decisiones con respecto a la seguridad de los activos de información.

INTRODUCCIÓN

En la actualidad la seguridad informática es un punto clave de análisis, puesto que las condiciones van cambiando a lo largo del tiempo de acuerdo a las nuevas tecnologías. La posibilidad de interconectarse a través de diversas redes, ha permitido ahondar en nuevos horizontes para conocer más allá de lo que podemos observar en nuestro país, dando como resultado esto, la aparición de nuevas amenazas tecnológicas que pudieran poner en riesgo nuestros activos de información.

Debido a lo anteriormente expuesto, muchas instituciones tanto públicas como privadas, han tomado en cuenta la necesidad de desarrollar documentos y directrices que indiquen el uso adecuado de las herramientas tecnológicas y recomendaciones para obtener el mayor beneficio de estas, y evitar el uso indebido de la mismas, lo cual puede traer como consecuencia serios problemas en los activos de la organización.

En este sentido, este trabajo de grado en donde se recomiendan políticas de seguridad informática para el Ministerio del Poder Popular para la Educación Superior, surge como una herramienta organizacional que debe hacer reflexionar a cada uno de los miembros de esta institución sobre la importancia y sensibilidad de la información y servicios críticos que permiten al Ministerio desarrollarse y mantenerse en sus labores diarias.

De acuerdo con lo anteriormente expuesto, el proponer o identificar una política de seguridad requiere un alto compromiso con el Ministerio del Poder Popular para la Educación Superior, así como destreza técnica para establecer fallas y debilidades, y perseverancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea a las organizaciones actuales.

Es importante señalar que estas políticas de seguridad deben ser enriquecidas y compatibilizadas con otras políticas dependientes de estas, objetivos de seguridad, procedimientos, etc. Debe estar fácilmente accesible de forma que todo el personal del Ministerio esté al tanto de su existencia y entiendan su contenido.

El presente trabajo de grado consiste en presentar el diseño de una metodología e implementación de políticas de seguridad en la red de comunicaciones del Ministerio del Poder Popular para la Educación Superior.

La estructura de este trabajo de grado se esquematiza en cinco capítulos:

CAPITULO I: Se describe el contexto del problema y su formulación. Se destaca la importancia del trabajo a realizar.

CAPITULO II: Se presenta lo que se ha considerado esencial conocer sobre la seguridad informática y los aspectos relacionados a la misma.

CAPITULO III: Se expone el marco metodológico en donde se explica al detalle los pasos a seguir para realizar este trabajo de grado, así como los aspectos más resaltantes de la metodología usada para llevar a cabo el análisis de riesgos de los activos de información.

1.

CAPITULO IV: Se expone el resultado obtenido después de aplicar la metodología de análisis de riesgo escogida, así como las políticas de seguridad que se deben implementar en el Ministerio del Poder Popular para la Educación Superior, y las recomendaciones adecuadas para hacer efectivas a las mismas.

RECOMENDACIONES: Se describen los pasos a seguir y los procedimientos más efectivos y eficientes para llevar a cabo la implementación de políticas de seguridad adecuadas.

CONCLUSIONES: Se exponen los logros y el alcance de las metas obtenidas a través de la elaboración del presente trabajo de grado.

CAPITULO I: EL PROBLEMA

SITUACIÓN ACTUAL DE LA RED DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN SUPERIOR

El Ministerio del Poder Popular para Educación Superior fue creado el 8 de Enero del 2002, con la finalidad de asesorar, formular y ejecutar políticas, planes y proyectos que permitan el mejoramiento de la calidad, la equidad y la pertinencia de la educación superior en la búsqueda permanente de la excelencia académica a partir de la evaluación continua de sus componentes, la existencia de un personal altamente calificado y una estructura organizativa de alta eficiencia y eficacia, sustentada en un modelo participativo y democrático, a fin de asegurar que la formación del talento humano en educación superior, tanto formal como no formal, esté en función de los requerimientos del desarrolb del país.

Este Ministerio cuenta con una estructura de 7 pisos, 2 sótanos y un edificio anexo de 2 platas adicionales, el centro de control de la institución está ubicado en el sótano 2, área donde residen los servidores propios de la institución y unos servicios anexos a los cuales se les da alojamiento en elmismo centro (Misión Sucre).

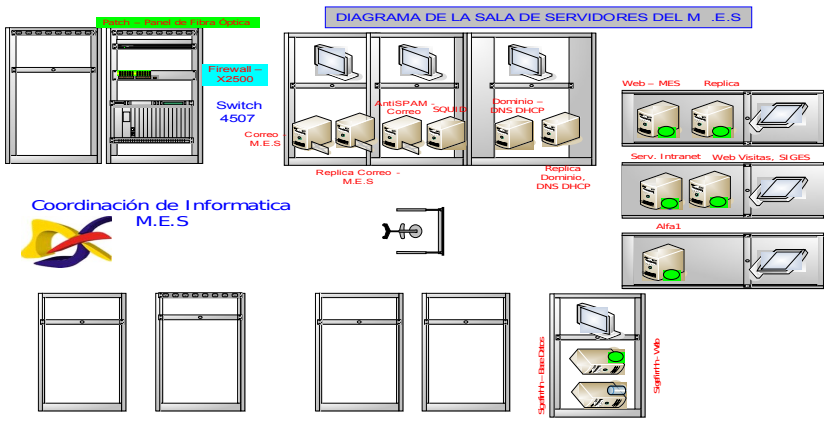

Figura Nro.1. Diagrama de la sala de servidores del Ministerio del Poder Popular para la Educación Superior

La plataforma de intercomunicación del edificio con el resto de los pisos, es mediante un backbone de fibra óptica, a ésta área también convergen los servicios del proveedor de Internet CNTI con un enlace de E1 (2.048 Mbps). Están en el mismo rack de servicio los equipos que resguardan la seguridad de la institución con la existencia de un firewall.

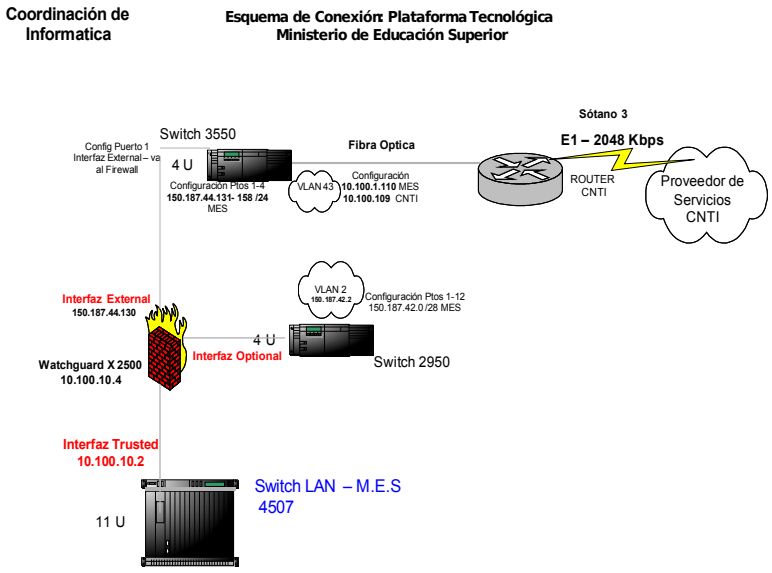

Figura Nro. 2. Esquema de conexión. Plataforma Tecnológica del Ministerio del Poder Popular para la Educación Superior

En cada piso está un cuarto de cableado estructurado Categoría 5e, que distribuye voz y datos debidamente organizados y perfectamente mantenidos. El direccionamiento de las direcciones IP en los pisos se estableció a través de la creación de una serie de redes locales virtuales (VLAN) por cada piso, dando un total de 7 VLAN y un ámbito por cada uno de ellos en el servidor DHCP

En cuanto a servidores el Ministerio tiene en unos un total de 10, los cuales presentan las siguientes características (Ver tabla Nro 1):

SERVIDORES	PLATAFORMA EN USO
SERVIDOR SQUID	LINUX (en su distribución Red Hat)
SERVIDOR SIGEFIRRHH	LINUX (en su distribución SUSE)
SERVIDOR WEB	LINUX (en su distribución Red Hat)
SERVIDOR ANTI-SPAM	LINUX (en su distribución Red Hat)
SERVIDOR DE CORREO	LINUX (en su distribución Red Hat)
SERVIDOR DE BASE DE DATOS SQL	Windows Server 2003.
SERVIDOR DE DOMINIO	Microsoft Windows Server 2003.
SERVIDOR ANTIVIRUS	Microsoft Windows XP
SERVIDORES DE MISION SUCRE	LINUX (en su Distribución Debian)
SERVIDOR DE CONTROL DE ACCESO	Microsoft Windows XP

Tabla Nro. 1. Características de los Servidores

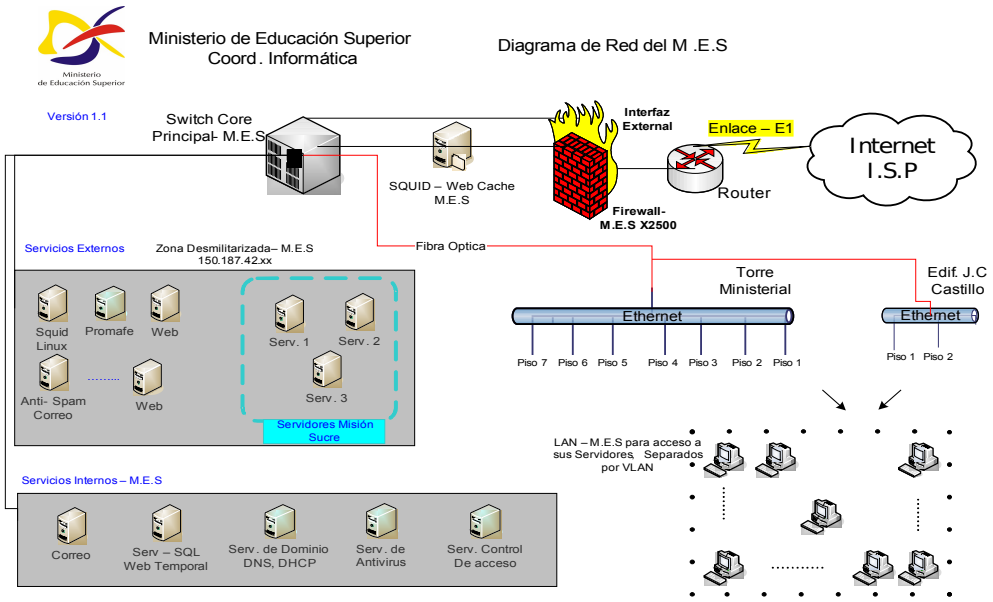

Figura Nro. 3. Configuración física de la red de datos del Ministerio del Poder Popular para la Educación Superior

Los componentes de la red, así como los servidores principales, se encuentran físicamente en un área acondicionada especialmente para asegurar su correcto funcionamiento, a la cual sólo tiene acceso el personal autorizado.

Todas las Direccciones y Coordinaciones del Ministerio tienen asignada un área de trabajo en los servidores, la cual tiene como objetivo fundamental almacenar y proteger la información relevante en cada una de las unidades involucradas. A estas áreas sólo tienen acceso empleados del departamento o de la coordinación correspondiente a la misma, con previa autenticación y control por parte del servidor. El proceso de respaldo de estas áreas es planificado por el administrador de redes, realizándose en algunos casos diariamente un respaldo completo y el resto de la semana uno incremental. En las estaciones de trabajo cada uno de los usuarios es responsable de reguardar su información ya que no existe una política de respaldo a estaciones de trabajo.

Es necesariamente importante destacar que las prácticas de seguridad establecidas actualmente en el Ministerio del Poder Popular para la Educación Superior no se encuentran documentadas, ni existen manuales que describan los procesos principales de éstas. A nivel estructural no existe ningún área orientada específicamente a desarrollar y mantener programas y políticas de seguridad de la información. A su vez, no se ha desarrollado una política de seguridad a seguir por el Ministerio, que sirva como base para la implementación y configuración de la red local. Las medidas existentes, en cuanto a estos aspectos, son resultado de iniciativas independientes de cada uno de los integrantes de la coordinación de Informática con previa autorización de la Dirección de Administración y Servicios.

El levantamiento de información y análisis realizados en materia de seguridad de la información, se han enfocado principalmente a la protección y seguridad física de los bienes en los cuales se procesa, almacena o transporta la información manejada por la empresa. Estos se han basado en la implementación de herramientas tecnológicas implantadas a nivel de la red, sin contar con un establecimiento claro y conciso de las políticas de seguridad necesarias para el Ministerio.

OBJETIVOS DEL PROYECTO

En vista de la situación planteada y a la falta de documentación actualizada sobre las políticas, normas, y procedimientos u otro tipo de mecanismos diseñados para garantizar la seguridad de la información, el Ministerio del Poder Popular para la Educación Superior se ha visto la necesidad de llevar a cabo un proyecto de seguridad de información, que contempla los siguientes objetivos:

- Elaborar un estudio de la seguridad de la información mediante la realización de un análisis de riesgos, con el objetivo de determinar los niveles de seguridad actuales dentro del Ministerio.
- Elaborar un análisis de deficiencias con basea los estándares del Ministerio.
- Revisión de Procedimientos en el manejo de la información y auditoría de configuración.
- Evaluación de las vulnerabilidades.
- Elegir herramientas ingeniosas adaptadas a sus necesidades que contengan las acciones preventivas y correctivas más eficaces y eficientes.
- Recomendar medidas de protección que contemplen las normas y procedimientos, con el objeto de incluir las mejores prácticas de acuerdo a las necesidades del Ministerio.

El alcance de estos objetivos permitirá ofrecer al Ministerio del Poder Popular para la Educación Superior soluciones en cuanto a seguridad de información que contemple todo lo referente a la red local y asentar las bases de diversas implementaciones a corto, mediano y largo plazo, tomando en cuenta que la información debe ser protegida de problemas de transformaciones indebidas, difusion no autorizada, eliminación y manejo no permitido.

CAPITULO II MARCO TEÓRICO

ANTECEDENTES

Desde el comienzo del uso de sistemas informáticos ha existido una gran preocupación por la seguridad de la información. Los responsables de los centros de cómputos se han encargado desde hace años de implantar controles de seguridad física frente a intrusos interesados en acceder a los sistemas, y han realizado periódicamente copias de seguridad para prevenir posibles pérdidas involuntarias de los datos.

La extensión de la informática y de las redes de ámbito mundial que interconectan recursos informáticos de todo tipo, ha hecho que los peligros que sufre la información almacenada en los diversos sistemas crezcan considerablemente y se diversifiquen, y que las medidas adoptadas internamente en los centros de datos resulten insuficientes.

En la actualidad, no sólo la prensa especializada en informática, sino todos los medios de difusión han hecho eco del futuro de las autopistas de la información, cuyo embrión está representado por la red Internet. A raíz de la interconexión del mundo empresarial a esta red, viaja por ella y se almacena información de todo tipo, que abarca desde noticias, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren medidas de seguridad que garanticen la confidencialidad, la integridad y la disponibilidad de los datos.

BASES TEÓRICAS

Una política de seguridad informática es un conjunto de reglas que definen la manera en que una organización maneja, administra, protege y asigna recursos para alcanzar el nivel de seguridad físico definido como objetivo.

Estas políticas de seguridad definen las decisiones relativas sobre los objetivos de la seguridad de la información; describen claramente de que se requiere proteger y fortalecer el eslabón más débil de la cadena de seguridad de la información.

Dentro de los objetivos de la seguridad informática encontraremos tres elementos claves como lo son:

- **Integridad:** El primero de los tres principios de la seguridad de la información que aplicamos es la integridad**,** la cual nos permite garantizar que la información no ha sido alterada en su contenido. Una información íntegra es una información que no ha sido alterada de forma indebida o no autorizada. Cuando ocurre una alteración no autorizada de la información en un documento, quiere decir que el documento ha perdido su integridad. La integridad de la información es fundamental para el éxito de la comunicación.

Una información se podrá alterar de varias formas, tanto su contenido como el ambiente que la soporta. Por lo tanto, la falta de integridad de la información se podrá considerar bajo dos aspectos:

1. Alteraciones del contenido de los documentos, donde se realizan inserciones, sustituciones o remociones de partes de su contenido;
2. Alteraciones en los elementos que soportan la información, donde se realizan alteraciones en la estructura física y lógica donde una información está almacenada.

Es importante resaltar que no se puede garantizar la integridad de la información, solo se puede detectar la pérdida de la información.

- **Confidencialidad**: El principio de la confidencialidad de la información tiene como propósito el asegurar que sólo la persona correcta acceda a la información correspondiente. La información que se intercambian entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos, y muchas veces a una única persona. Eso significa que estos datos deberán ser conocidos sólo por un grupo controlado de personas, definido por el responsable de la información. Por ese motivo, se dice que la información posee un grado de confidencialidad que se deberá preservar para que personas sin autorización no la conozcan. Tener confidencialidad en la comunicación, es la seguridad de que lo que se dijo a alguien o escribió en algún lugar será escuchado o leído sólo por quien tenga ese derecho.

Si una información es confidencial, se deberá guardar con seguridad y no ser divulgada para personas no autorizadas. Garantizar la confidencialidad es uno de los factores determinantes para la seguridad y una de las tareas más difíciles de implementar, pues involucra a todos los elementos que forman parte de la comunicación de la información, desde su emisor, el camino que ella recorre, hasta su receptor. Y también, cuanto más valiosa es una información, mayor debe ser su grado de confidencialidad. Y cuanto mayor sea el grado de confidencialidad, mayor será el nivel de seguridad necesario de la estructura tecnológica y humana que participa de este proceso: del uso, acceso, tránsito y almacenamiento de las informaciones.

Se deberá considerar a la confidencialidad con base en el valor que la información tiene para la empresa o la persona y los impactos que podría causar su divulgación indebida. Siendo así, debe ser accedida, leída y alterada sólo por aquellos individuos que poseen permisos para tal. Por lo tanto, se debe mantener la integridad de una información, según el principio básico de la seguridad de la información.

- **Disponibilidad**: Una vez que nos aseguramos que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que debemos garantizar es que llegue en el momento oportuno**,** y precisamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad. Para que una información se pueda utilizar, deberá estar disponible. Este principio se refiere a la disponibilidad de la información y de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento.

La disponibilidad de la información permite que:

- Se utilice cuando sea necesario.
- Que esté al alcance de sus usuarios y destinatarios autorizados.
- Se pueda accederla en el momento en que necesitan utilizarla.

Este principio está asociado a la adecuada estructuración de un ambiente tecnológico y humano que permita la continuidad de los negocios de la empresa o de las personas, sin impactos negativos para la utilización de la información No basta estar disponible: la información deberá estar accesible a únicamente a usuarios permitidos en forma segura para que se pueda usar en el momento en que se solicita y que se garantice su integridad y confidencialidad. Así, el ambiente tecnológico y los soportes de la información deberán estar funcionando correctamente y en forma segura para que la información almacenada en los mismos y que transita por ellos pueda ser utilizada por los usuarios permitidos.

DEFINICIÓN DE TÉRMINOS

A continuación de definen algunos conceptos concernientes a la seguridad de información:

Activo: Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta su receptor.

Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.

Son tres elementos que conforman lo que denominamos activos:

- La información,
- Los Equipos que la soportan y,
- Las personas que los utilizan.

CLASIFICACIÓN DE LOS ACTIVOS

La clasificación de los activos viene dada de acuerdo a los siguientes criterios:

- Información
- Equipos que la soportan: software y hardware.
- Organización
- Personas que los utilizan o usuarios:

Información: En este grupo están los elementos que contienen información almacenada en medios electrónicos o físicos. Entre los más importantes tenemos por

ejemplo documentos, informes, libros, manuales, correspondencias, patentes, información de mercado, código de programación, líneas de comando, reportes financieros, archivos de configuración, planillas de sueldos de empleados, plan de negocios de una empresa, etc.

Posibles vulnerabilidades: Robo de documentos, pérdida de archivos de configuración, entre otros.

Software: Este grupo de activos contiene todos los programas de computación que se utilizan para la automatización de procesos, es decir, acceso, lectura, tránsito y almacenamiento de la información. Entre ellos citamos: las aplicaciones comerciales, desarrollos propios, sistemas de operaciones, entre otros.

La seguridad de la información busca evaluar la forma en que se crean las aplicaciones, cómo están colocadas a disposición y la forma en que son utilizadas por los usuarios y por otros sistemas, para detectar y corregir problemas existentes en la comunicación entre ellos.

Las aplicaciones deberán estar protegidas para que la comunicación entre las bases de datos, otras aplicaciones y los usuarios se realice de forma segura, atendiendo a los principios básicos de la seguridad de la información. Ejemplos de este tipo de activos: sistemas operativos (Unix, Windows, Linux, etc.), programas de correo electrónico, bases de datos, aplicaciones específicas, sistemas de respaldo entre otros. **Posibles vulnerabilidades:** Fallas publicadas de los sistemas operativos y las aplicaciones no reparadas pueden representar accesos indebidos a los equipos. Son entradas usadas por hackers y virus.

Hardware: Estos activos representan toda la infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento. Los activos que pertenecen a este grupo son: Cualquier equipo en el cual se almacene, procese o transmita la información de la empresa. Ejemplos de este tipo de activos: las computadoras, los servidores, los equipos portátiles, los mainframes, los medios de

almacenamiento, los equipos de conectividad, enrutadores, switches y cualquier otro elemento de una red de computadoras por donde transita la información. **Posibles vulnerabilidades:** Fallas eléctricas que dañen los equipos, inundaciones en centros de cómputos, robo de equipos portátiles.

Organización: En este grupo se incluyen los aspectos que componen la estructura física y organizativa de las empresas. Se refiere a la organización lógica y física que tiene el personal dentro de la empresa en cuestión. Como ejemplos de estructura organizativa, tenemos entre otros: la estructura departamental y funcional, el cuadro de asignación de funcionarios, la distribución de funciones y los flujos de información de la empresa. En lo que se refiere al ambiente físico, se consideran entre otros: salas y armarios donde están localizados los documentos, como por ejemplo: sala de servidores de archivos, entre otros. **Posibles vulnerabilidades:** Ubicación insegura de documentos, equipos o personas. Estructura organizacional que no permita los cambios en materia de seguridad.

Usuarios: El grupo usuarios se refiere a los individuos que utilizan la estructura tecnológica y de comunicación de la empresa y que manejan la información. El enfoque de la seguridad en los usuarios, está orientado hacia la toma de conciencia de formación del hábito de la seguridad para la toma de decisiones y acción por parte de todos los empleados de una empresa, desde su alta dirección hasta los usuarios finales de la información, incluyendo los grupos que mantienen en funcionamiento la estructura tecnológica, como los técnicos, operadores y administradores de ambientes tecnológicos. Ejemplos de este tipo de activos: Empleados del área de contabilidad, directivos de la empresa. **Posibles vulnerabilidades**: No usar contraseñas complejas, no bloquear la computadora, falta de cooperación por parte de los usuarios en materia de seguridad, descuido de parte de los usuarios en el manejo de la información, robo de información.

Amenazas: Las amenazas son agentes capaces de explotar los fallos de seguridad que denominamos puntos débiles y como consecuencia de ello, causar

pérdidas o daños a los activos de una empresa, afectando sus negocios. Los activos están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas siempre existirán y están relacionadas a causas que representan riesgos, las cuales pueden ser:

- Causas naturales o no naturales
- Causas internas o externas

Por lo tanto, entendemos que uno de los objetivos de la seguridad de la información es impedir que las amenazas exploten puntos débiles y afecten alguno de los principios básicos de la seguridad de la información (integridad, disponibilidad, confidencialidad) causando daños al negocio de las empresas.

Las amenazas son constantes y pueden ocurrir en cualquier momento. Esta relación de frecuencia-tiempo, se basa en el concepto de riesgo, lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil. Las mismas se podrán dividir en tres grandes grupos:

1. Amenazas naturales: condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos.

2. Intencionales: son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.

3. Involuntarias: son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

“Entre las principales amenazas, la ocurrencia de virus, la divulgación de contraseñas y la acción de hackers están entre las más frecuentes”.

Puntos débiles: Las amenazas siempre han existido y es de esperarse que conforme avance la tecnología. También surgirán nuevas formas en las que la información puede llegar a estar expuesta. Por tanto es importante conocer el marco general de cómo se clasifican las vulnerabilidades o puntos débiles que pueden hacer que esas amenazas impacten nuestro sistemas, comprometiendo los principios de la seguridad de nuestra información. Los puntos débiles son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa. Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información.

Al ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

Los puntos débiles dependen de la forma en que se organizó el ambiente en que se maneja la información. La existencia de puntos débiles está relacionada con la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma se está utilizando.

Vulnerabilidad: En términos de Seguridad de la Información, una vulnerabilidad es una debilidad en los procedimientos de seguridad, diseño, implementación o control interno que podría ser explotada (accidental o intencionalmente) y que resulta en una brecha de seguridad o una violación de la política de seguridad de sistemas.

Entre los tipos de vulnerabilidades se pueden señalar las siguientes:

- **Vulnerabilidades físicas:** Los puntos débiles de orden físico son aquellos presentes en los ambientes en los cuales la información se está almacenando.

Estos puntos débiles, al ser explotados por amenazas, afectan directamente los principios básicos de la seguridad de la información, principalmente la disponibilidad.

- **Vulnerabilidades naturales**: Los puntos débiles naturales son aquellos relacionados con las condiciones de la naturaleza que puedan colocar en riesgo la información. Muchas veces, la humedad, el polvo y la contaminación podrán causar daños a los activos. Por ello, los mismos deberán estar protegidos para poder garantizar sus funciones. La probabilidad de estar expuestos a las amenazas naturales es determinante en la elección y montaje de un ambiente. Se deberán tomar cuidados especiales con el local, de acuerdo con el tipo de amenaza natural que pueda ocurrir en una determinada región geográfica. Entre las amenazas naturales más comunes podemos citar: ambientes sin protección contra incendios, locales próximos a ríos propensos a inundaciones, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes etc.

- **Vulnerabilidades de hardware:** Los posibles defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos. Existen muchos elementos que representan puntos débiles de hardware. Entre ellos podemos mencionar: la ausencia de actualizaciones conforme con las orientaciones de los fabricantes de los programas que se utilizan, y conservación inadecuada de los equipos. Por ello, la seguridad de la información busca evaluar:
    1. Si el hardware utilizado está dimensionado correctamente para sus funciones.
    2. Si posee área de almacenamiento suficiente, procesamiento y velocidad adecuados.

  La falta de configuración de respaldos o equipos de contingencia pudiera representar una vulnerabilidad para los sistemas de la empresa.

- **Vulnerabilidades de software:** Los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red. Los puntos débiles relacionados con el software podrán ser explotados por diversas amenazas ya conocidas. Entre éstos destacamos: La configuración e instalación indebidas de los programas de computadora, que podrán llevar al uso abusivo de los recursos por parte de usuarios mal intencionados. A veces la libertad de uso implica el aumento del riesgo. Ejemplo: Lectores de e-mail que permiten la ejecución de códigos maliciosos, editores de texto que permiten la ejecución de virus de macro etc. Estos puntos débiles colocan en riesgo la seguridad de los ambientes tecnológicos.

  Las aplicaciones son los elementos que realizan la lectura de la información y que permiten el acceso de los usuarios a dichos datos en medio electrónico y, por esta razón, se convierten en el objetivo predilecto de agentes causantes de amenazas. También podrán tener puntos débiles de aplicaciones los programas utilizados para la edición de texto e imagen, para la automatización de procesos y los que permiten la lectura de la información de una persona o empresa, como los navegadores de páginas del Internet.

  Los sistemas operativos como Microsoft ® Windows ® y Unix ®, que ofrecen la interfaz para configuración y organización de un ambiente tecnológico. Estos son el blanco de ataques, pues a través de los mismos se podrán realizar cualquier alteración de la estructura de una computadora o red.

  Estas aplicaciones son vulnerables a varias acciones que afectan su seguridad, como por ejemplo la configuración e instalación inadecuada, ausencia de actualización, programación insegura, etc.

- **Vulnerabilidades de medios de almacenaje:** Los medios de almacenamiento son los soportes físicos o magnéticos que se utilizan para almacenar la información. Entre los tipos de soporte o medios de almacenamiento de la información que están expuestos podemos citar: disquetes, dvd, cd, cintas magnéticas, discos duros de los servidores y de las bases de datos, así como lo que está registrado en papel. Si los soportes que almacenan información, no se utilizan de forma adecuada, el contenido en los mismos podrá estar vulnerable a una serie de factores que podrán afectar la integridad, disponibilidad y confidencialidad de la información.

  Los medios de almacenamiento podrán ser afectados por puntos débiles que podrán dañarlos e incluso dejarlos indispuestos. Entre estos puntos débiles, destacamos los siguientes: plazo de validez y caducidad, defecto de fabricación, uso incorrecto, lugar de almacenamiento en locales insalubres o con alto nivel de humedad, magnetismo o estática, moho, etc.

- **Vulnerabilidades de comunicación:** Este tipo de punto débil abarca todo el tránsito de la información. Donde sea que la información transite, ya sea vía cable, satélite, fibra óptica u ondas de radio, debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información. Hay un gran intercambio de datos a través de medios de comunicación que rompen barreras físicas tales como teléfono, Internet, WAP, fax, etc. Siendo así, estos medios deberán recibir tratamiento de seguridad adecuado con el propósito de evitar que: cualquier falla en la comunicación haga que una información quede no disponible para sus usuarios, o por el contrario, estar disponible para quien no posee derechos de acceso. Ejemplo: La información sea alterada en su estado original, afectando su integridad, La información sea capturada por usuarios no autorizada, afectando su confidencialidad. Por lo tanto, la seguridad de la información también está asociada con el desempeño de los equipos involucrados en la comunicación, pues se preocupa por: la calidad del ambiente que fue preparado para el tránsito,

tratamiento, almacenamiento y lectura de la información. Ejemplo: La ausencia de sistemas de encriptación en las comunicaciones que pudieran permitir que personas ajenas a la organización obtengan información privilegiada, La mala elección de sistemas de comunicación para envío de mensajes de alta prioridad de la empresa pudiera provocar que no alcanzaran el destino esperado o bien se interceptara el mensaje en su tránsito.

- **Vulnerabilidades humanas:** Esta categoría de vulnerabilidad está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta. Los puntos débiles humanos también pueden ser intencionales o no. Muchas veces, los errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales. La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por cada elemento constituyente, principalmente los miembros internos de la empresa. Destacamos dos puntos débiles humanos por su grado de frecuencia:

    - La falta de capacitación específica para la ejecución de las actividades inherentes a las funciones de cada uno,
    - La falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones etc.

  En lo que se refiere a las vulnerabilidades humanas de origen externo, podemos considerar todas aquéllas que puedan ser exploradas por amenazas como: vandalismo, estafas, invasiones, etc. Ejemplo: Contraseñas débiles, falta de uso de criptografía en la comunicación, compartimiento de identificadores tales como nombre de usuario o credencial de acceso, entre otros.

INGENIERÍA SOCIAL

En éste punto es muy importante señalar un concepto muy usado hoy en día como lo es la ingeniería social, la cual no es más que la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o el Internet para engañar a la gente y llevarla a revelar información considerada como sensible o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar los agujeros de seguridad en los sistemas de información. Generalmente se está de acuerdo en que los usuarios son el punto más débil en seguridad; éste es el principio por el que se rige la ingeniería social.

Básicamente la ingeniería social es todo artilugio, tretas y técnicas más elaboradas a través del engaño de las personas en revelar contraseñas u otra información, más que la obtención de dicha información a través de las debilidades propias de una implementación y mantenimiento de un sistema.

El único medio para entender como defenderse contra esta clase de ataques es conocer los conceptos básicos que pueden ser utilizados contra usted o su compañía y que abren brechas para conseguir sus datos.

Ataque: Se puede definir como ataque en seguridad de información a todo método por el cual, valiéndose de una vulnerabilidad y sin tener el permiso correspondiente, o sin validarse o identificarse, se puede realizar una negación de servicio, ejecutar código arbitrario, obtener información confidencial, escalar privilegios, administrar el sistema, tomar el control, etc.

Entre los tipos de ataques se pueden considerar los siguientes:

- **Ataques de intromisión:** Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su

interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

- **Ataque de espionaje en líneas:** Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.

- **Ataque de interceptación:** Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en unared.

- **Ataque de modificación:** Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y base de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad del los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.).

- **Ataque de negación de servicio:** Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos

anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

- **Ataque de suplantación:** Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjeta de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Figura Nro. 4. Diagrama de Vulnerabilidades.

Riesgos: El riesgo es la probabilidad de que las amenazas exploten los puntos débiles**,** causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: la confidencialidad, la integridad y la disponibilidad de la información. Se puede concluir entonces que la seguridad es una práctica orientada hacia la eliminación de las vulnerabilidades para evitar o reducir la posibilidad que las potenciales amenazas se concreten en el ambiente que se quiere proteger. El principal objetivo es garantizar el éxito de la comunicación segura, con información disponible, íntegra y confidencial, a través de medidas de seguridad que puedan tornar factible el negocio de un individuo o

empresa con el menor riesgo posible.

Medidas de seguridad: Las medidas de seguridad son acciones orientadas hacia la eliminación de vulnerabilidades, teniendo en mira evitar que una amenaza se vuelva realidad. Estas medidas son el paso inicial para el aumento de la seguridad de la información en un ambiente de tecnología de la información y deberán considerar el todo. Ya que existe una variedad de clases de puntos débiles que afectan la disponibilidad, confidencialidad e integridad de la información, deberán existir medidas de seguridad específicas para el tratamiento de cada caso.

Antes de la definición de las medidas de seguridad a ser adoptadas, se deberá conocer el ambiente en sus mínimos detalles, buscando los puntos débiles existentes. A partir de este conocimiento, se toman las medidas o acciones de seguridad que pueden ser de índole:

- Preventivo: buscando evitar el surgimiento de nuevos puntos débiles y amenazas;
- Perceptivo: orientado hacia la revelación de actos que pongan en riesgo la información.
- Correctivo: orientado hacia la corrección de los problemas de seguridad conforme su ocurrencia.

Las medidas de seguridad son un conjunto de prácticas que, al ser integradas, constituyen una solución global y eficaz de la seguridad de la información. Entre las principales medidas se destacan: Análisis de riesgos, Política de seguridad, especificación de seguridad, Administración de seguridad.

La seguridad de la información debe ser garantizada en una forma integral y completa de ahí que resulte de mucha utilidad conocer con un poco más de detalle estas cuatro medidas de seguridad que permiten movernos desde el análisis de riesgos hasta la administración de la seguridad:

Política de seguridad: Es una medida que busca establecer los estándares de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos. Es una forma de suministrar un conjunto de normas para guiar a las personas en la realización de sus trabajos. Es el primer paso para aumentar la conciencia de la seguridad de las personas, pues está orientada hacia la formación de hábitos, por medio de manuales de instrucción y procedimientos operativos.

Especificación de seguridad: Son medidas que tienen en mira instruir la correcta implementación de un nuevo ambiente tecnológico, por medio del detalle de sus elementos constituyentes y la forma con que los mismos deben estar dispuestos para atender a los principios de la seguridad de la información.

Administración de la seguridad: Son medidas integradas para producir la gestión de los riesgos de un ambiente. La administración de la seguridad involucra a todas las medidas mencionadas anteriormente, en forma preventiva, perceptiva y correctiva, con base en el ciclo de la seguridad que se explica a continuación.

Ciclo de Seguridad de la Información: El ciclo de seguridad se inicia con la identificación de las amenazas a las cuales están sometidas las empresas. La identificación de las amenazas permitirá la visualización de los puntos débiles que se podrán explotar, exponiendo los activos a riesgos de seguridad. Esta exposición lleva a la pérdida de uno o más principios básicos de la seguridad de la información, causando impactos en el negocio de la empresa, aumentando aún más los riesgos a que están expuestas las informaciones. Para que el impacto de estas amenazas al negocio se pueda reducir, se toman medidas de seguridad para impedir la ocurrencia de puntos débiles.

Así, se concluye la definición de seguridad de la información desde la ilustración del ciclo:

Figura Nro. 5. Ciclo de Seguridad de Información.

Como podemos ver en al figura anterior, los riesgos en la seguridad de la empresa aumentan en la medida que las amenazas pueden explotar las vulnerabilidades, y por tanto causar daño en los activos. Estos daños pueden causar que la confidencialidad, integridad o disponibilidad de la información se pierda, causando impactos en el negocio de la empresa.

Las medidas de seguridad permiten disminuir los riesgos, y con esto, permitir que el ciclo sea de mucho menor impacto para los activos, y por tanto, para la empresa. Por lo tanto, la seguridad es una actividad cuyo propósito es: proteger a los activos contra accesos no autorizados, evitar alteraciones indebidas que pongan en peligro su integridad garantizar la disponibilidad de la información y es instrumentada por medio de políticas y procedimientos de seguridad que permiten: la identificación y control de amenazas y puntos débiles, teniendo en mira la preservación de la confidencialidad, integridad y disponibilidad de la información.

Análisis de riesgos: Es una medida que busca rastrear vulnerabilidades en los activos que puedan ser explotados por amenazas. El análisis de riesgos tiene como resultado un grupo de recomendaciones para la corrección de los activos para que los mismos puedan ser protegidos.

El análisis de riesgos es un paso importante para implementar la seguridad de la información. Como su propio nombre lo indica, es realizado para detectar los riesgos a los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.

Las amenazas se pueden convertir en realidad a través de fallas de seguridad, que conocemos como vulnerabilidades y que deben ser eliminadas al máximo para que el ambiente que se desea proteger esté libre de riesgos de incidentes de seguridad. Por lo tanto, la relación entre amenaza-incidente-impacto, es la condición principal a tomar en cuenta en el momento de priorizar acciones de seguridad para la corrección de los activos que se desean proteger y deben ser siempre considerados cuando se realiza un análisis de riesgos. (Ver figura Nro. 6).

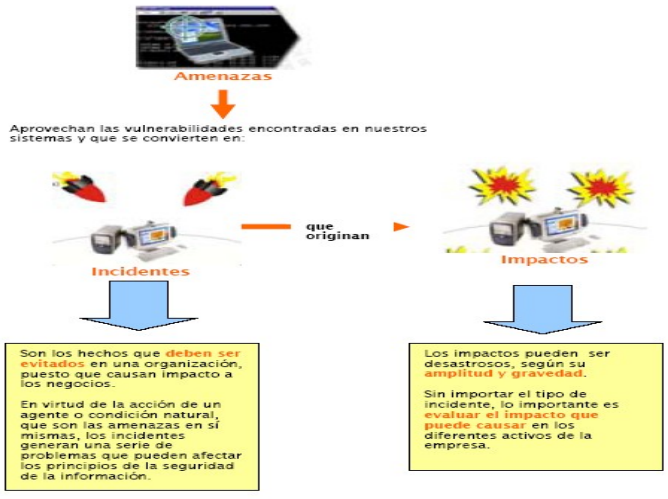

Figura Nro. 6. Esquema de relación: amenaza-incidente-impacto.

Definiciones de análisis de Riesgo:

- Una actividad centrada en la identificación de fallas de seguridad que evidencien vulnerabilidades que puedan ser explotadas por amenazas, provocando impactos en los negocios de la organización.
- Una actividad de análisis que pretende, a través del rastreo, identificar los riesgos a los cuales los activos se encuentran expuestos.
- Encontrar la consolidación de las vulnerabilidades para identificar los pasos a seguir para su corrección.
- Identificar las amenazas que pueden explotar esas vulnerabilidades y de esta manera se puede llegar a su corrección o eliminación.
- Identificar los impactos potenciales que pudieran tener los incidentes y de esta forma aprovechar las vulnerabilidades encontradas.
- El análisis de riesgos es además una actividad que tiene por resultado: Determinar las recomendaciones para que las amenazas sean corregidas o reducidas.

Otro punto importante a considerar en la realización del análisis de riesgos es la relación costo-beneficio. Este cálculo permite que sean evaluadas las medidas de seguridad con relación a su aplicabilidad y el beneficio que se agregará al negocio. Así, esta visión orienta la implementación de las medidas de seguridad sólo en las situaciones en que la relación costo-beneficio se justifique. Sin embargo, es fundamental que en la organización esté clara la relación costo beneficio, es decir, que todos aquellos involucrados en la implementación de la seguridad (el equipo de ejecución del proyecto, la alta administración y todos sus usuarios) deben estar conscientes de los beneficios que las medidas de seguridad traerán para los individuos

y para la organización como un todo.

Momento de análisis de riesgos: El análisis de riesgos puede ocurrir antes o después de la definición de una política de seguridad. Según la norma internacional BS/ISO/IEC 17799, esta actividad puede ser hecha después de la definición de la política. El propósito de tomar en cuenta una política de seguridad en el análisis se debe a varias razones:

- La política de seguridad delimita el alcance del análisis.
- Permite ser selectivo en la verificación de activos que la política establece como vulnerables.
- El análisis toma en cuenta la lista de amenazas potenciales que la misma política contempla.

Para tener más claro porqué decimos que la definición de una política de calidad marca el momento para iniciar un análisis de riesgos de la seguridad de la información recordemos qué es política de seguridad:

Política de seguridad: Es una medida que busca establecer las directrices de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos. Es una forma de suministrar un conjunto de normas internas para guiar la acción de las personas en la realización de sus trabajos. Es el primer paso para aumentar la conciencia de la seguridad de las personas, pues está orientada hacia la formación de hábitos, por medio de manuales de instrucción y procedimientos operativos. Sin embargo, la realización del análisis de riesgos como primer elemento de la acción de seguridad, es un hecho determinante para procesos críticos en que son analizadas todas las amenazas. De esta manera son considerados y analizados todos los activos de la organización, sea por muestreo o en su totalidad, para que estén libres de vulnerabilidades con el propósito de reducir los riesgos. Por esta razón serán abordados en esta parte todos los elementos necesarios para la realización de un análisis de riesgos como etapa de búsqueda de vulnerabilidades de todo el ambiente de un proceso de

negocios. Para tener más clara esta relación revisemos unos ejemplos concretos de cada uno de los factores:

- **Valor alto o alta exposición de los bienes afectados**: En una empresa de asesores en contabilidad, los activos comúnmente afectados son las bases de datos con las auditorias de sus clientes, y por tanto, son de alto valor para la compañía y sus negocios.

- **Históricamente los bienes atacados son afectados**: En una empresa se tienen estadísticas de que los servidores que han sido atacados por virus o hackers siempre resultan dañados en su información o configuración y esto ocasiona perjuicios en las operaciones de la compañía.

- **Factores atenuantes**: Si por ejemplo, sabemos que los activos que comúnmente son atacados en la empresa no poseen un alto valor para los negocios de la misma

- **Bajo riesgo**: Los activos que comúnmente en la empresa se catalogan como de bajo riesgo son por citar alguno, las estaciones de trabajo que no manejan o almacenan información vital para los negocios.

Ámbitos para la realización del análisis de riesgos: Además de conocer el momento y duración adecuada para la realización de nuestro análisis de riesgos, es importante también estar concientes de los diferentes ámbitos en los que podemos aplicar dicho análisis. El análisis de riesgos puede ser realizado en distintos ámbitos. Por lo general, todos son considerados, puesto que la implementación de seguridad pretende corregir el entorno en que se encuentra la información. Entre los ámbitos conocidos se tiene:

- **Ámbito tecnológico**: El análisis de riesgos realizado en el entorno tecnológico pretende el conocimiento de las configuraciones y de la disposición topológica de los activos de tecnología que componen toda la infraestructura de respaldo de la información para comunicación, procesamiento, tránsito y almacenamiento. **Aspectos por analizar**: Los activos son de tipo aplicación y equipo, sin dejar de considerar también la sensibilidad de las informaciones que son manipulados por ellos. Los usuarios que los utilizan. La infraestructura que les ofrece respaldo.

- **Ámbito humano**: El análisis de riesgos también se destina a la comprensión de las maneras en que las personas se relacionan con los activos. Así, es posible detectar cuáles vulnerabilidades provenientes de acciones humanas, se encuentran sometidos los activos, y es posible dirigir recomendaciones para mejorar la seguridad en el trabajo humano y garantizar la continuidad de los negocios de la organización. Este análisis pretende inicialmente identificar vulnerabilidades en los activos de tipo usuario y organización. **Aspectos por analizar**: El nivel de acceso que las personas tienen en la red o en las aplicaciones. Las restricciones y permisos que deben tener para realizar sus tareas con los activos. El nivel de capacitación y formación educativa que necesitan tener acceso para manipularlos, etc.

- **Ámbito de procesos**: Análisis de los flujos de información de la organización y la manera en que la información transita de un área a otra, cómo son administrados los recursos en relación a la organización y manutención. De esta manera, será posible identificar los eslabones entre las actividades y los insumos necesarios para su realización con el objetivo de identificar las vulnerabilidades que puedan afectar la confidencialidad, la disponibilidad y la integridad de la información y en consecuencia, del negocio de la organización. En este ámbito, el activo de enfoque principal es del tipo usuario e información. **Aspectos**

por analizar: Identificar a las personas involucradas en el flujo de información, es posible evaluar la necesidad real de acceso que ellas tienen a los activos. Evaluar el impacto proveniente del uso indebido de la información por personas no calificadas.

- **Ámbito físico**: El análisis físico de seguridad pretende identificar en la infraestructura física del ambiente en que los activos encuentran vulnerabilidades que puedan traer algún perjuicio a la información y a todos los demás activos. El enfoque principal de este ámbito de análisis son los activos de tipo organización, pues son los que proveen el soporte físico al entorno en que está siendo manipulada la información. **Aspectos por analizar**: Identificar posibles fallas en la localización física de los activos tecnológicos. Evaluar el impacto de accesos indebidos a las áreas en donde se encuentran activos tecnológicos. Evaluar el impacto de desastres ambientales en la infraestructura de tecnología de la empresa.

CAPITULO III. MARCO METODOLÓGICO

Para llevar a cabo este Trabajo Especial de Grado se usaron como referencias las normas ISO 17799:2005 e ISO 27001 además de una Metodología de desarrollo de Proyectos suministrada por la Coordinación de Informática del Ministerio del Poder Popular para La Educación Superior, como guía para hacer el estudio de la problemática planteada al principio de este trabajo y establecer la solución más eficaz y eficiente. En el contexto del Ministerio, el análisis y diseño del proyecto se refirió a estudiar su situación actual en el área de seguridad de las redes de telecomunicaciones, con el objeto de optimizarla con métodos y procedimientos más eficientes.

Lo primero que se llevó a cabo para el estudio de la situación actual de la seguridad de la red del Ministerio del Poder Popular para la educación Superior fue una etapa de **Investigación Preliminar**. En esta etapa se definen y establecen los objetivos del proyecto, incluyendo el establecimiento de la solución conceptual y los costos preliminares de éste. Se buscó la información necesaria con respecto al problema o situación, para estudiar la factibilidad de que este trabajo sea de utilidad para el Ministerio del Poder Popular para la Educación Superior. A continuación se se explican las actividades que integran esta etapa:

PRIMERA ETAPA: INVESTIGACIÓN PRELIMINAR

- **Objetivo**: Documentar los objetivos del área al cual está dirigido el Proyecto.
- **Identificación del Problema**: Establecer las necesidades y los requerimientos del proyecto.
- **Información Preliminar**: Investigación de aspectos conceptuales relacionados con el proyecto.
- **Planificación del Proyecto**: Establecer la necesidad de los recursos y la información para llevar a cabo satisfactoriamente el proyecto.

- **Alcances del proyecto**: Establecer las limitaciones del proyecto y delimitaciones de sus actividades.
- **Descripción del Proyecto**: Definir las características de la solución propuesta.

La segunda etapa es la **Determinación de Requerimientos**; es esta fase es muy importante la intervención del usuario final, para optimizar la definición específica de los requerimientos para el desarrollo y evaluación de la solución conceptual propuesta. Se hizo un estudio de los métodos de operación del sistema de seguridad de información del Ministerio, para establecer dónde era necesario llevar a cabo mejoras, así como las diversas metodologías estratégicas para satisfacer los requerimientos fundamentales, obtenidos como resultado en la investigación preliminar. En esta etapa se investigaron los detalles necesarios para proponer las estrategias de seguridad de la información, estudiando la situación actual con la ayuda de varias herramientas (entrevistas, cuestionarios, etc), lo que permitió observar el desempeño de la estrategia de seguridad actual y su relación con las necesidades del Ministerio del Poder Popular para la Educación Superior Las actividades llevadas a cabo en esta etapa fueron:

SEGUNDA ETAPA: DETERMINACIÓN DE LOS REQUERIMIENTOS

- **Investigación de situaciones similares**: En esta fase se hace el estudio de situaciones similares en proyectos anteriores, para poder definir algun tipo de información que suministre algún tipo de orientación para la solución conceptual propuesta.
- **Análisis de la Información**: En esta fase se analizan los aspectos técnicos que se obtienen como resultado de la etapa anterior y expresarlo en la planificación del Proyecto.
- **Descripción del Area de Trabajo**: En ésta fase se explica hacia que área especificamente va dirigido el proyecto de investigación, con la finalidad de ofrecer mejoras en el área.
- **Requerimientos Finales del Proyecto**: Definir los recursos necesarios así

como el establecimiento de actividades para establecer los requerimientos finales del proyecto.

Luego de llevar a cabo las fases anteriores, se seleccionaron las estrategias que serían utilizadas para alcanzar los requerimientos establecidos, en la etapa denominada **Diseño Detallado,** lo cual permitió establecer y complementar los métodos para estimar la seguridad de información dentro del Ministerio, además de establecer los procedimientos que deben llevarse a cabo al usar las redes de información del Ministerio. Las actividades integradas en esta fase son:

TERCERA ETAPA: DISEÑO DE LA ESTRUCTURA DE LA INFORMACIÓN

Esquematizar al detalle los datos e informaciones necesarias para llevar a cabo el proyecto.

- **Especificaciones**: Fomentar especificaciones detalladas al proyecto con la finalidad de hacer una buena distribución de las asignaciones.
- **Material de Apoyo**: Idear las secuencias operacionales necesarias para llevar a cabo el proyecto exitosamente.
- **Plan de Implementación**: Planear la estrategia a seguir, detallando actividades necesarias para la implementación del proyecto.
- **Diseño Técnico**: Cotejar los requerimientos técnicos y las ventajas del proyecto para asegurar que son usados los métodos adecuados.

A continuación se llevó a cabo la fase de **Desarrollo o Aplicación**, en la cual se explica el desarrollo de las actividades enunciadas en la etapa de diseño. En esta actividad se aplica la metodología de análisis de riesgos MAGERIT y se detallan las medidas y controles necesarios, en cuanto a herramientas y políticas. Esta etapa estará culminada cuando los productos definidos en las etapas de requerimiento y diseño hayan sido desarrollados y probados. Las fases a seguir son las siguientes:

CUARTA ETAPA: DESARROLLO O APLICACIÓN

- **Integración de Actividades**: Verificar que las actividades precisadas en la estrategia funcionen como un todo y cumplan objetivos diferentes que complementen la solución del problema.
- **Aplicación de la Estrategia**: Idear las actividades y procesos necesarios para implementar el proyecto.
- **Prueba Individual**: localizar y corregir errores identificados en la implementación del proyecto.
- **Documentación de Resultados**: Documentar el resultado obtenido de las tareas ejecutadas, con la finalidad de comprobar la solución del problema

Investigación Preliminar: La tarea inicial de esta fase incluyó la investigación bibliográfica relacionada con la seguridad de las redes y sus basamentos teóricos. En esta etapa, también se llevaron a cabo los primeros contactos con los usuarios finales, a través de reuniones con algunos Directores del Ministerio del Poder popular para la Educación Superior, para recolectar los datos iniciales para la investigación. Estos datos fueron obtenidos a través de entrevistas informales, que permitieron obtener información general de Ministerio de forma directa.

Con el objetivo de establecer las necesidades del Ministerio en cuanto a la seguridad de la información, fue sumamente necesario analizar detalladamente las metas que se ha trazado la Institución. Para esto se llevaron a cabo entrevistas a diferentes personas en distintas Direcciones, con la finalidad de identificar:

- Necesidades de seguridad de Activos de Información.
- Misión y visión de la empresa.
- Prioridades y delimitaciones de seguridad.
- Tecnología de información utilizada

Esta investigación sirvió como primera fase para poder involucrarse con las

actividades de la institución en cuanto al desempeño de sus tareas. Las necesidades de seguridad de activos de información identificadas, determinaron la necesidad de proteger integralmente la información que maneja el Ministerio. Esta necesidad sale a flote debido a que la Institución mantiene relaciones con diversas Universidades, Institutos y Colegios Universitarios a nivel nacional, por lo tanto requiere manejar con cuidado la información confidencial o clasificada, ya que muchas de las actividades que se realizan pueden conllevar al uso o la divulgación de información confidencial a través de sus redes.

Muchas de las actividades llevadas a cabo en el Ministerio del Poder Popular para la Educación Superior tienen que ver con el procesamiento de datos y uso de equipos de computación, ya que la mayoría de los empleados usan computadoras y el software instalado en cada una de ellas, por lo que es de vital importancia vigilar y proteger el uso de estos recursos.

Para la obtención de soluciones que harían mas fácil el desarrollo de procedimientos eficaces que ayuden a proteger dichos recursos, se efectuaron revisiones preliminares de herramientas inteligentes para, luego, escoger aquellas que garantizarían la consistencia de las normas y procedimientos, al recomendar medidas de protección. A esta fase se le dedicó un tiempo considerable, haciendo notar que si se tomaban decisiones certeras con respecto a las herramientas correctas, se ahorrarían recursos en cuanto a personal, tiempo y dinero.

En esta etapa de investigación preliminar se estudiaron algunos productos y servicios que ya se utilizaban en la Institución, como parte del estudio de la situación actual. En cuanto a los servidores, se encuentran bajo las distribuciones de Linux Red Hat, Suse, y Debian, además de algunos con Windows 2003 y Windows 2000 Server. Para las estaciones de trabajo en su mayoría se encuentran con Windows XP Professional, sin embargo ya se encuentran algunos equipos instalados con Ubuntu y Debian.

El Ministerio de Poder Popular para la Educación Superior cuenta con una estructura de 7 pisos, 2 sótanos y un edificio anexo de 2 plantas adicionales, el centro de control de la institución esta ubicado en el Sótano 2, área donde residen los servidores propios de la institución y unos servicios anexos a los cuales se les da alojamiento en el mismo centro, (Misión Sucre).

La plataforma de intercomunicación del edificio con el resto de los pisos, es mediante un backbone de fibra óptica, a esta área también convergen los servicios del proveedor del Internet (CNTI) con un enlace de E1 (2048 Mbps). Están en mismo rack de servicio los equipos que resguardan la seguridad de la institución con la existencia de un firewall.

En cada piso esta un cuarto de cableado estructurado Cat 5e, que distribuye voz y datos debidamente organizados y perfectamente mantenidos.

Para comenzar con estas actividades se efectuó una primera reunión con el administrador de la red del Ministerio, a fin de obtener el soporte y fluidez de la información necesaria para recabar la mayor cantidad de información con relación al proyecto.

Luego se realizó una inspección con la más cordial de las actitudes y mucha colaboración por parte del personal del Ministerio.

En general los cuartos de cableado están en muy buena condición, se mantiene la organización, la identificación de los extremos de los patch cord de conexión, las tapas y organizadores del rack, se encuentran en sus sitios, hay existencia de aterramiento en los rack, están colocados los UPS de protección eléctrica, los racks cuentan adicionalmente con sus regletas de protección, la iluminación es buena, la ventilación presenta deficiencias; los equipos activos están bien anclados a los rack, pero no poseen identificación; la bandeja de fibra óptica esta en buena condición; el aterramiento en las tomas eléctricas de pared no esta del todo bien segura; los

detectores de incendio deben ser verificados; la seguridad del área aun cuando es controlada por el número de personas que pueden y tiene autorización, es irregular; no en todos los cuartos de cableados poseen comunicación telefónica.

Con respecto al centro de cómputos (ubicado en el sótano 2 de la Torre), las medidas de seguridad son más estrictas, existe doble seguridad (2 puertas metálicas), con acceso controlado; se tiene instalado sistema de vigilancia filmado con una cámara Web; control de acceso de visitantes. Es importante destacar que no cuentan con personal de operaciones en esta área.

Los tableros eléctricos se encontraron sin identificación de los breakers, sin identificación de seguridad alto voltaje y sin la tapa. El detector de incendios está físicamente, pero no esta activo. El aire acondicionado es deficiente en todas las áreas. En el edificio anexo, los tableros eléctricos están al lado del cuartode cableado.

Despues de levantar la información anterior y para llevar a cabo éste proyecto satisfactoriamente, se utilizaron fuentes de búsqueda tales como Internet, libros y revistas especializadas. Luego, se procedió a leer y revisar el material de los productos que fueron encontrados, para luego ordenarlos según los servicios que prestan y evaluar los aspectos concretos que servirían de utilidad para el Ministerio.

Entre los productos investigados se encuentran:

- **Firewall watchguard modelo X2500**, para controlar los accesos internos y externos a la red.
- Sistemas operativos como **Linux** en sus distribuciones **Debian, Red hat, Suse y Ubuntu y Windows 2000 y 2003 Server.**
- Cabe destacar que hasta el momento no se han adquirido los correspondientes software de monitoreo y administración de redes, los cuales son estrictamente necesarios, para poder realizar un análisis adecuado de los servicios dentro de la red y

establecer adecuadamente el comportamiento del ancho de banda de la misma, para así brindar mejores alternativas para optimizar el rendimiento en todos los servicios informáticos que se brindan a través de la infraestructura de red, así que también se hicieron investigaciones de algunos productos para monitoreo y administración de redes como el Observer, Ethereal , Iris, entre otros.

Debido a lo extenso del proceso del análisis y a que en ésta fase no se tenía un conocimiento profundo de la arquitectura de la red de la empresa, era muy arbitrario establecer consideraciones finales y definir con exactitud la problemática planteada. Por lo tanto, en esta etapa, se efectuó solo un análisis preliminar de estas herramientas, para luego tomarlo en consideración al momento de hacer las recomendaciones sobre las medidas de protección informáticas que complementaran la efectividad de las políticas de seguridad del Ministerio.

Determinación de Requerimientos: En la etapa anterior se recogieron los detalles preliminares relacionados con la plataforma de seguridad de información del Ministerio. Se estudiaron las características del mismo, en base a las referencias teóricas analizadas anteriormente (Capítulo II) y la experiencia de personas en áreas similares al que se encuentra en investigación.

En la etapa de determinación de requerimientos, se hicieron investigaciones sobre puntos más concretos orientados a brindar un mayor entendimiento del entorno de seguridad de información en el Ministerio del Poder Popular para la Educación Superior, para así obtener una descripción detallada de la situación actual. Las técnicas de recolección de información empleadas para recopilar los datos relacionados con los requerimientos fueron cuestionarios, entrevistas y la observación.

Se realizaron entrevistas con guía y cuestionarios a Directores, coordinadores

de areas y empleados seleccionados, por sus conocimientos en el área. Estas personas proporcionaron datos cualitativos esenciales para la investigación, tales como opiniones, descripciones de actividades y problemas.

Al Administrador de la red de datos del Ministerio del Poder Popular para la Educación Superior se le realizó una entrevista informal con la finalidad de conocer las funciones principales de ese departamento y las características de las operaciones computacionales manejadas por el Ministerio. Su información permitió establecer las responsabilidades en cuanto a la seguridad de la información e identificar posibles áreas de mejora en el departamento.

Además se aplicaron cuestionarios, a algunos departamentos del Ministerio, para obtener opiniones y experiencias generales en cuanto a la seguridad de la información de la institución. Los cuestionarios aplicados fueron los siguientes:

- **Políticas de Seguridad** (ver anexo 1): este cuestionario fue realizado a diferentes directores y coordinadores de areas con el objetivo de establecer la existencia de una política de seguridad estructurada y conocer sus características.

- **Organización de la Seguridad de la Información** (ver anexo 2): este cuestionario engloba preguntas relacionadas a la cooperación entre organizaciones, revisión independiente de la Seguridad de la Información, identificación de riesgos por el acceso de terceros, requerimientos de seguridad en contratos con terceros, y requerimientos de seguridad en contratos de externalización.

- **Gestión de Activos** (Ver anexo 3): este cuestionario engloba preguntas relacionadas al inventario de activos, guías de clasificación y marcado y

tratamiento de la información.

- **Seguridad de Recursos Humanos** (Ver anexo 4): este cuestionario engloba preguntas relacionadas a la comunicación de las incidencias de seguridad, comunicación de las debilidades de seguridad, comunicación de los fallos del software, aprendiendo de las incidencias, procedimientos disciplinarios.

- **Seguridad Física y ambiental** (Ver anexo 5): este cuestionario engloba preguntas relacionadas al mantenimiento de equipos, seguridad de equipos fuera de los locales de la organización, seguridad en la reutilizacion o eliminacion de equipos, politica de puesto de trabajo despejado y bloqueo de pantalla y sustracciones.

- **Gestión de comunicaciones y las operaciones** (Ver anexo 6): este cuestionario engloba preguntas relacionadas a la seguridad en comercio electrónico, seguridad del correo electrónico, seguridad de los sistemas ofimáticos, disponibilidad de los sistemas públicos y otras formas de intercambio de información.

- **Control de acceso** (Ver anexo 7): este cuestionario engloba preguntas relacionadas a el análisis y especificaciones de los requerimientos de seguridad, validación de los datos de entrada, control del proceso interno, autenticación de mensajes, validación de los datos de salida, política de uso de los controles criptográficos, cifrado, firmas digitales, servicios de no repudio, gestión de claves, control del software en explotación, protección de los datos de prueba del sistema, control de acceso a la librería de programas fuente, procedimientos de control de cambios, revisión técnica de los cambios en el sistema operativo, restricciones en los cambios a los paquetes de software, canales encubiertos y código

troyano y desarrollo externalizado del software.

- **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información** (Ver anexo 8): este cuestionario engloba preguntas relacionadas al aislamiento de sistemas sensibles, registro de incidencias, seguimiento del uso de los sistemas, sincronización de relojes, informática móvil y teletrabajo.

- **Gestión de la Continuidad Comercial** (Ver anexo 9): este cuestionario engloba preguntas relacionadas al proceso de gestión de la continuidad de negocio, continuidad del negocio y análisis de impacto, redacción e implantación de planes de continuidad, marco de planificación para continuidad del negocio, prueba, mantenimiento y revaluación de los planes de continuidad, contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

- **Conformidad** (Ver anexo 10): este cuestionario engloba preguntas relacionadas a los controles de auditoría de sistemas y la protección de las herramientas de auditoría de sistemas.

Para recolectar información adicional, se empleó la técnica de observación. Esta técnica permitió determinar la forma en que se manejan los documentos y se llevan a cabo los procesos de seguridad dentro del Ministerio, mediante la establecimiento de los siguientes criterios:

- Comportamiento de los empleados en cuanto a la seguridad de la información.
- Acceso al Centro de Procesamiento de Datos.

- Identificación visible del carnet de todos los empleados.
- Identificación de personas invitadas.
- Actitud del personal de Informática, en cuanto a la seguridad de la información.

De acuerdo a lo obtenido durante la recopilación de la información, se encontraron situaciones como la falta de una unidad dedicada a la seguridad de la información y de un manual de normas, políticas y procedimientos, así como el desconocimiento de las medidas de control vigentes por parte de muchos de los empleados, los cuales influyen considerablemente en la problemática de la inseguridad de la información. Basándonos en los resultados obtenidos, se llegó a la conclución que, entre otras cosas, la falta de una cultura de seguridad y la no definición de los riesgos a los que se expone el Ministerio del Poder Popular para la Educación Superior, producidos por el ambiente externo e interno.

Por lo anteriormente expuesto, se debió crear una política de seguridad de red, por lo cual fue importante que la idea de crear una política es asegurar que los esfuerzos llevados a cabo en la seguridad serán útiles. Esto significó conocer cuáles recursos de la red era necesario proteger, que algunos recursos son más importantes que otros, e identificar de quién y cómo deben ser protegidos.

También fué necesario elaborar un análisis de riesgos para determinar los puntos vulnerables del sistema y seleccionar soluciones que minimizaran los riesgos a un nivel considerable, permitiendo recomendar un plan de seguridad donde se asignan las responsabilidades para ciertas funciones y tareas con el fin de mejorar la seguridad.

Para cubrir los requerimientos establecidos, se elaboró una investigación acerca de las metodologías utilizadas para efectuar un análisis de riesgos, en busca de aspectos comunes con los objetivos del análisis a realizar. Se observó que el Ministerio no dispone de una metodología específica a seguir que contemple el análisis de riesgos de activos de información, razón por la cual de acuerdo al estudio de varias metodologías

como por ejemplo NTP 328, MAGERIT versión 2, OCTAVE, HAZOP, entre otras existentes, se determinó como la mas adecuada la metodología MAGERIT versión 2, el cual es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas", por ser ésta la metodología una de las más adaptable a los sistemas de Información que se encuentran en el Ministerio del Poder Popular para la educación superior, además contener aspectos comunes con los objetivos del análisis a realizar en éste trabajo.

MAGERIT es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. Esta metodología ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática (España).

Diseño Detallado: El objetivo fundamental de esta etapa estuvo dirigido a proporcionar una estrategia, que contrastara los acontecimientos encontrados en las dos etapas anteriores de la metodología con la teoría investigada en el Capítulo de Marco Teórico. Para este fin, se consideraron todos los procedimientos que integraran los requerimientos identificados y especificaran las nuevas medidas de protección en cuanto a la seguridad de información que debían incorporarse el Ministerio del Poder Popular para la Educación Superior, en función de producir las mejoras o cambios que cumplieran con las condiciones previamente establecidas. La estrategia que se define contempló inicialmente la realización de un análisis de riesgos, para luego efectuar recomendaciones de la política de seguridad que incluyera los recursos, normas y procedimientos conjuntamente con la selección de medidas de protección tecnológicas, que definieran el nuevo ambiente de seguridad de la empresa. los siguientes puntos definen la estrategia que se ha seguido:

- Análisis de Riesgos.
- Recomendación de Políticas de Seguridad.
- Selección de Medidas de seguridad.
- Implementación de Medidas y Controles.
- Revisión de Efectividad.

Figura Nro. 7. Análisis de gestión de riesgos en su contexto

METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología utilizada para alcanzar los objetivos de éste trabajo es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas **MAGERIT**

MAGERIT como metodología para el análisis y gestión de riesgos de los sistemas de información persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la

existencia de riesgos y de la necesidad de atajarlos a tiempo.

- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Apoyar la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación,según corresponda en cada caso.
- En esta fase se expone de forma conceptual en qué consiste esto del análisis de riesgos y aquello de su gestión, qué se busca en cada momento y qué conclusiones se derivan.

Hay dos grandes tareasa realizar:

- **Análisis de Riesgos**, que permite determinar qué tiene la organización y estimar lo que podría pasar.

Elementos:

- Activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con éste) que aportan valor a la Organización.
- Amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la organización.
- Salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen (tanto) daño.

Con estos elementos se puede estimar:

- El impacto: lo que podría pasar

- El riesgo: lo que probablemente pase.

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

- **Gestión de riesgos**, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume. Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

Análisis de Riesgos: El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

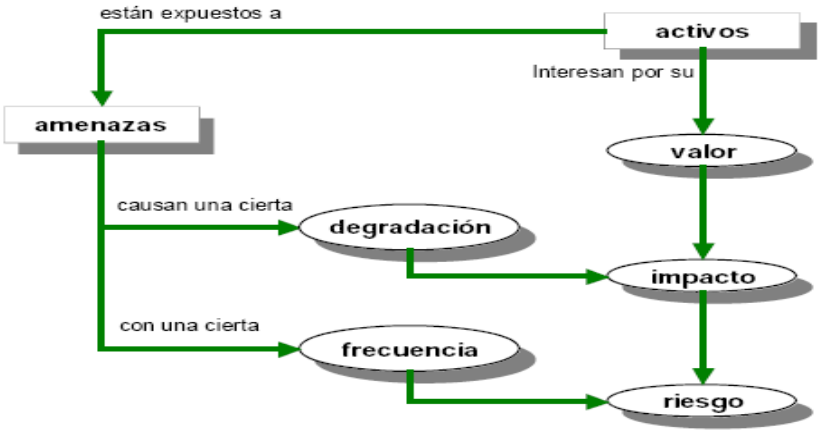

Figura Nro. 8. Fases del Análisis de Riesgos de acuerdo a la Metodología MAGERIT

Paso 1: Activos

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.

- Las personas que explotan u operan todos los elementos anteriormente citados.

Tipos de activos: No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes. Si el sistema maneja datos de carácter personal, estos suelen ser importantes por sí mismos y requerir una serie de salvaguardas frecuentemente reguladas por ley. En estos activos interesa determinar qué tratamiento hay que imponerles. El hecho de que un dato sea de carácter personal impacta sobre todos los activos involucrados en su tratamiento y custodia.

Algo similar ocurre con los datos sometidos a una clasificación de confidencialidad. Cuando se dice que un cierto informe está clasificado como "reservado", de forma que las copias están numeradas, sólo pueden llegar a ciertas personas, no deben salir del recinto y deben ser destruidas concienzudamente, etc. se están imponiendo una serie de salvaguardas porque lo ordena el reglamento, sectorial o específico de la Organización.

Dependencias: Los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones o las frecuentemente olvidadas personas que trabajan con aquellos. Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo superior se verá afectado por un incidente de seguridad en un activo inferior.

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

Capa 1: El Entorno: activos que se precisan para garantizar las siguientes capas:

- Equipamiento y suministros: energía, climatización, comunicaciones.
- Personal: de dirección, de operación, de desarrollo, etc.
- Otros: edificios, mobiliario, etc.

Capa 2: El sistema de información propiamente dicho:

- Equipos informáticos (hardware).
- Aplicaciones (software).
- Comunicaciones.
- Soportes de información: discos, cintas, etc.

Capa 3: La Información:

- Datos.
- Meta-Datos: estructuras, índices, claves de cifra, etc.

Capa 4: Las funciones de la Organización, que justifican la existencia del sistema de información y le dan finalidad:

- objetivos y misión.
- Bienes y servicios producidos.

Capa 5: Otros activos

- Credibilidad o buena imagen.
- Conocimiento acumulado.

- Independencia de criterio o actuación.
- Privacidad de las personas.
- Integridad física de las personas.

Valoración: ¿Por qué interesa un activo? Por lo que vale. No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información (o datos) que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de datos y servicios finales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

Dimensiones: De un activo puede interesar calibrar diferentes dimensiones:

- Su autenticidad: ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar).
- Su confidencialidad: ¿Qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.

- Su integridad: ¿Qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- Su disponibilidad: ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

En sistemas dedicados a la administración electrónica o al comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. En estos activos, además de la autenticidad, interesa calibrar la:

a) La trazabilidad del uso del servicio: ¿Qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
b) La trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Se reconocen habitualmente las dimensiones básicas: autenticidad, confidencialidad, integridad y disponibilidad. En esta metodología se ha refinado la autenticidad para distinguir entre el uso de un servicio y el acceso a unos datos. Además se ha introducido el concepto de trazabilidad tomado de las guías ISO/IEC 13335, igualmente segmentada entra la trazabilidad del servicio y la de los datos. Los aspectos de autenticidad y trazabilidad de los datos son críticos para satisfacer medidas reglamentarias sobre ficheros que contengan datos de carácter personal.

¿Cuánto vale la "salud" de los activos? Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del costo que supondrá salir de una incidencia que destruirá el activo. Hay muchos factores a considerar:

1) Coste de reposición: adquisición e instalación.
2) Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo.

3) Lucro cesante: pérdida de ingresos.
4) Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
5) Sanciones por incumplimiento de la ley u obligaciones contractuales.
6) Daño a otros activos, propios o ajenos.
7) Daño a personas.
8) Daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

1) La homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.
2) La relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos.

Todos estos criterios se satisfacen con valoraciones económicas (coste monetario requerido para "curar" el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente.

Valoración cualitativa: Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "Órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Valoración cuantitativa: Las valoraciones numéricas absolutas cuestan mucho

esfuerzo; pero no adolecen de los problemas de las valoraciones cualitativas. Sumar valores numéricos es absolutamente "natural" y la interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es monetaria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

1) ¿Vale la pena invertir tanto dinero en esta salvaguarda?

2) ¿Qué conjunto de salvaguardas optimizan la inversión?
3) ¿En qué plazo de tiempo se recupera la inversión?
4) ¿Cuánto es razonable que cueste la prima de un seguro?

El valor de la interrupción del servicio: Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad. No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño o moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

Paso 2: Amenazas: El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño. Hay accidentes naturales (terremotos, inundaciones, entre otros) y desastres industriales (contaminación, fallos eléctricos, entre otros) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados. No todas las amenazas afectan a todos los activo, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas: Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar que tan vulnerable es el activo, en dos sentidos:

- Degradación: Que tan perjudicado resultará el activo.
- Frecuencia: cada cuánto se materializa la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable. La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos.

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

Tabla Nro. 2. Frecuencia de ocurrencia de un evento

Paso 4: Determinación del impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Impacto acumulado: Es el calculado sobre un activo teniendo en cuenta:

1) El valor acumulado (el propio más el acumulado de los activos que dependen de él).
2) las amenazas a que está expuesto.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Impacto repercutido: Es el calculado sobre un activo teniendo en cuenta:

1. su valor propio.
2. Las amenazas a que están expuestos los activos de los que depende.

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio de un activo. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado. El impacto

repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de valores de impacto: Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

1) Puede agregarse el impacto repercutido sobre diferentes activos,
2) Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común,
3) No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,
4) Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
5) Puede agregarse el impacto de una amenaza en diferentes dimensiones.

Paso 5: Determinación del riesgo: Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

Riesgo acumulado: Es el calculado sobre un activo teniendo en cuenta:

1) El impacto acumulado sobre un activo debido a una amenaza.
2) La frecuencia de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo repercutido: Es el calculado sobre un activo teniendo en cuenta:

a) El impacto repercutido sobre un activo debido a una amenaza.
b) La frecuencia de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza. El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de riesgos: Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

1) Puede agregarse el riesgo repercutido sobre diferentes activos.
2) Puede agregarse el riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común.
3) No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.
4) Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.

5) Puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Paso 3: Salvaguardas: En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes. Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal.

Las salvaguardas entran en el cálculo del riesgo de dos formas:

1) Reduciendo la frecuencia de las amenazas. Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.
2) Limitando el daño causado. Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

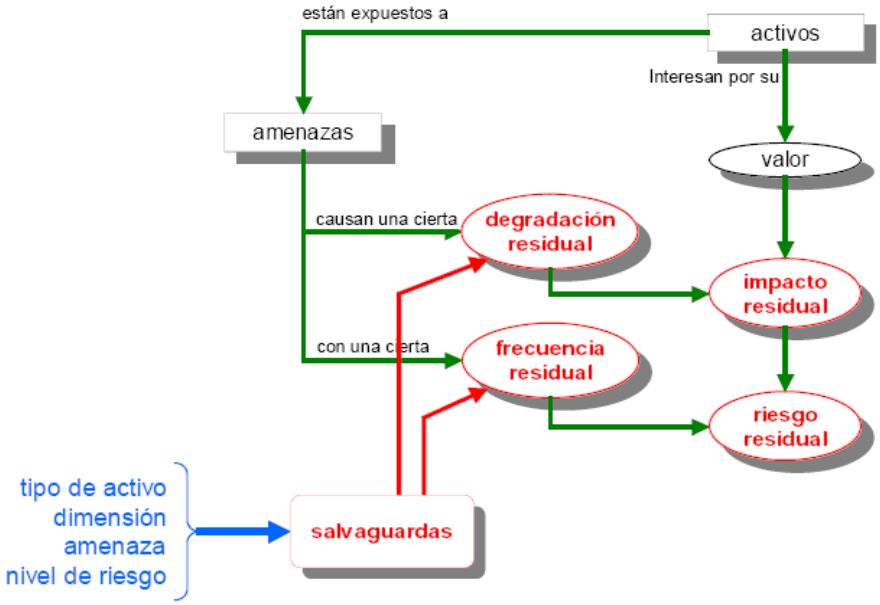

Figura Nro. 9. Degradación, frecuencia, impacto y riesgo residual.

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, lo que implica que:

- Es teóricamente idónea.
- Está perfectamente desplegada, configurada y mantenida.
- Se emplea siempre.
- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

Revisión del paso 4: impacto residual: Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable. Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación. La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Revisión del paso 5: riesgo residual Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable. Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia. La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la frecuencia tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Gestión de Riesgos: El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se de la circunstancia. En cambio el riesgo pondera la probabilidad de que

ocurra. El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable. Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo.

La interpretación de los valores de impacto y riesgo residuales: Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer. Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza.

Mientras el valor residual sea más que despreciable, hay una cierta exposición.

Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de Insuficiencias.

Selección de salvaguardas: Las amenazas hay que conjurarlas, por principio y mientras no se justifique lo contrario. Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades). Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

1. Establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada

cosa.

2. Establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada.
3. Establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer.
4. Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas.
5. Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto.

A este conjunto de elementos se le encasilla habitualmente bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando.

El párrafo anterior puede llamar a engaño si el lector interpreta que hay que llevar a cabo todos y cada uno de los puntos para cada amenaza. No. En la práctica lo dicho se traduce en desarrollar una política, unas normas y unos procedimientos junto con el despliegue de una serie de salvaguardas y controles y, ahora sí verificar que todas y cada una de las amenazas tienen una respuesta adecuada.

De los puntos anteriores, el más "abierto" es el de determinación de las salvaguardas apropiadas. Es realmente un arte que requiere personal especializado aunque en la práctica las situaciones más habituales están perfectamente documentadas en la literatura y basta elegir de entre un catálogo en función de la magnitud del riesgo.

Tipos de salvaguardas: Un sistema debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea despreciable. Es decir, impedir incidentes o ataques. En la práctica, no todo es previsible, ni todo lo previsible es económicamente razonable atajarlo en sus orígenes.

Tanto para enfrentar lo desconocido como para protegerse de aquello a lo que se

permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza impidiendo que se convierta en un desastre. Tanto las medidas preventivas como las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer por último de medidas de recuperación que devuelvan el valor perdido por los activos.

Es de sentido común intentar actuar de forma preventiva para que las cosas no puedan ocurrir o no puedan causar mucho daño; pero no siempre es posible y hay que estar preparados para que ocurran. Lo que no debe ser de ninguna manera es que un ataque pase inadvertido: hay que detectarlo, registrarlo y reaccionar primero con un plan de emergencia (que pare y limite el incidente) y después con un plan de continuidad y recuperación para regresar a donde se debe estar.

Por último, hay que recordar que conviene llegar a un cierto equilibrio entre:

- salvaguardas técnicas: en aplicaciones, equipos y comunicaciones.
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos.
- Medidas de organización: de prevención y gestión de las incidencias.
- política de personal: que, a fin de cuentas, es el eslabón imprescindible y más delicado: política de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

Pérdidas y ganancias: Es de sentido común que no se puede invertir en salvaguardas más allá del valor de los propios activos a proteger.

Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

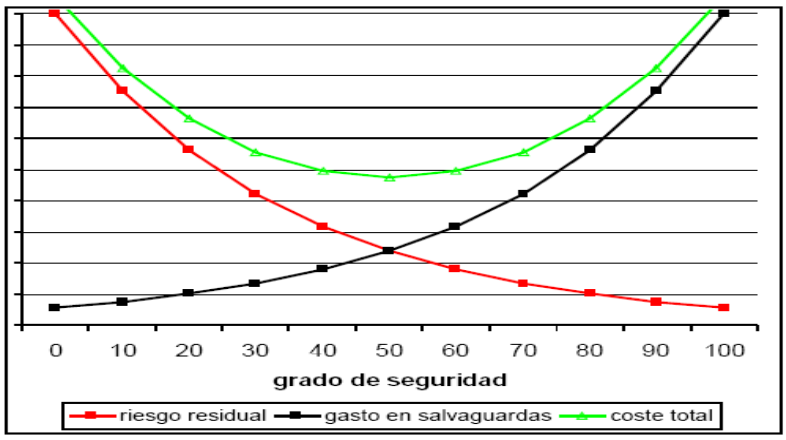

Figura Nro. 10. Grado de Seguridad

Este tipo de gráficas intentan reflejar cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones y que el costo de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%

La curva central suma el costo para la Organización, bien derivado del riesgo (baja seguridad), bien derivado de la inversión en protección. De alguna forma existe un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa, punto al que hay que tender si la única consideración es económica

Pero llevar el sentido común a la práctica no es evidente, ni por la parte del cálculo del riesgo, ni por la parte del cálculo del coste de las salvaguardas. En otras palabras, la curva anterior es conceptual y no se puede dibujar en un caso real. En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos:

- E0: si no se hace nada
- E1: si se aplica un cierto conjunto de salvaguardas
- E2: si se aplica otro conjunto de salvaguardas

Y así N escenarios con diferentes combinaciones de salvaguardas. El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (no hacer nada) una opción posible, que pudiera estar justificada económicamente. En cada escenario hay que estimar a lo largo del tiempo el coste que va a suponer. Para poder agregar costes, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero. Considerando los siguientes componentes:

- (recurrente) riesgo residual
- (una vez) coste de las salvaguardas
- (recurrente) coste anual de mantenimiento de las salvaguardas
- (recurrente) mejora en la productividad
- (recurrente) mejoras en la capacidad de la organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

El escenario E0 es muy simple: todos los años se afronta un gasto marcado por el riesgo, que se acumula año tras año. Si la frecuencia de las amenazas se ha estimado como tasa anual, los datos de riesgo residual estarían automáticamente anualizados. Si se hubiera empleado otra escala, habría que convertirla a términos anuales.

Si la salvaguarda ya existe, costo de mejora. Si no existiera, costo de adquisición e instalación. En cualquier caso hay que imputar costes de formación de los operadores, usuarios, etc.

Lo anteriormente expuesto puede ser positivo si la organización si mejora su productividad; o puede ser negativo, si empeora. Como ejemplo típico de salvaguardas

que mejoran la productividad podemos citar la introducción de dispositivos de autenticación en sustitución de la clásica contraseña. Como ejemplo típico de salvaguardas que minoran la productividad podemos citar la clasificación de documentación con control de acceso restringido. En los demás escenarios, hay cosas que suman y cosas que restan, pudiendo darse varias situaciones:

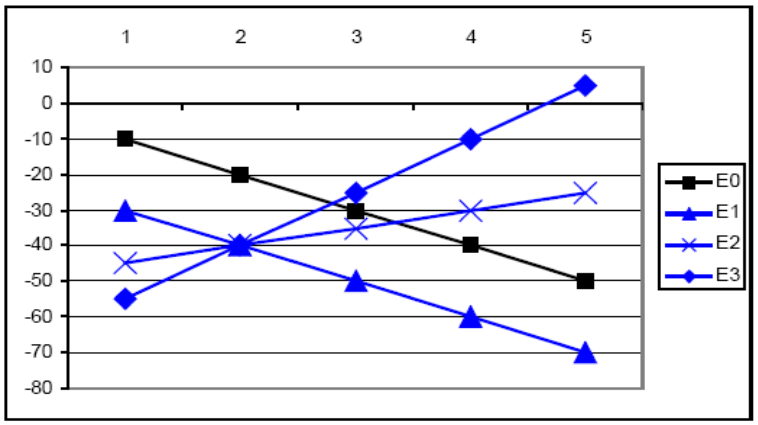

Figura Nro. 11. Valor de salvaguarda

La actitud de la Dirección: La dirección de la organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias.

Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, entre otros). Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección.

Si el impacto y/o el riesgo están por encima de lo aceptable, se puede:

1) Eliminar el activo; suena muy fuerte, pero a veces hay activos que,

simplemente, no vale la pena mantener.

2) Introducir nuevas salvaguardas o mejorar la eficacia de las presentes.

Revisión del paso 1: activos: Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos activos soportan parte del valordel sistema y están a su vez sujetos a amenazas que pueden perjudicar a los activos de valor.

Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la organización.

Desarrollo o Aplicación: Esta fase permitió establecer y complementar los métodos para evaluar la seguridad de información dentro del Ministerio del poder Popular para la Educación Superior, además de permitir el establecimiento de los procedimientos que deben llevarse a cabo al usar las redes de información.

POLÍTICAS DE SEGURIDAD DE LA RED

Para construir medidas de protección efectivas, se desarrolló un documento que pretende recomendar procedimientos y planes, que salvaguarden los recursos de la red de del Ministerio del Poder Popular para la Educación Superior contra pérdidas y daños. Estas políticas de seguridad de la red del Ministerio contemplaron diversos aspectos, desde la administración de seguridad de la red hasta la conducta de los usuarios que la utilizan y de esta manera, establecer formalmente la definición de los criterios y lineamientos a seguir en esta materia. Para ello, se tomaron encuenta gran variedad de factores técnicos, humanos y culturales relacionados con las características propias de la Administración Pública.

Inicialmente, para crear la política de seguridad, se llevaron a cabo las pautas expuestas en el Capítulo de Análisis de Fundamentos Conceptuales, acerca de cómo idear y establecer una política de seguridad. Con esta documentación, y luego de analizar tanto la situación actual del Ministerio como los resultados obtenidos del análisis de riesgos, se contaron con los siguientes aspectos iniciales para desarrollar la política de seguridad de la empresa:

- Activos y recursos a proteger.
- Ataques de los cuales es necesario proteger los recursos.
- Factibilidad de las amenazas.
- Importancia de los recursos y activos.
- Medidas a implantar para proteger los bienes de una manera económica y factible

Estos aspectos permitieron identificar todos los recursos a los cuales su seguridad está en riesgo de ser violentada, las posibles amenazas a estos recursos y la factibilidad de su puesta en marcha. Se determinó la prioridad de los activos a proteger y algunas de las medidas de protección en contra de los eventos adversos, elementos que sirvieron como inicio para determinar los asuntos que debían ser contemplados en cuanto al uso de la red y sus responsabilidades, para establecer dentro de las políticas lo siguiente:

- Usuarios con permiso de utilizar los recursos
- Uso correcto de los recursos
- Personal autorizado para garantizar acceso y aprobar el uso
- Privilegios de administración del sistema
- Derechos y responsabilidades del usuario
- Derechos y responsabilidades del administrador del sistema frente a los usuarios
- Derechos y responsabilidades de la alta gerencia

Después de establecer a qué usuarios se les permite ingresar a los recursos de la red, se debieron documentar las guías para el uso aceptable de los mismos. Estas guías dependen de la clase de usuario: usuario interno o externo. Por esto, en la política se establece qué tipo de uso de red es aceptable e inaceptable y qué tipo de uso será restringido.

En las políticas de seguridad, la responsabilidad de cada usuario influye en los mecanismos de seguridad implantados. En muchos casos, dentro de la política recomendada, se plantea claramente cómo debe ser la conducta a seguir por los empleados, para evitar consecuencias legales a la institución, relacionadas con empleados que indiquen que no se les informó o entrenó acerca de la política de red. La siguiente es una lista de restricciones que fueron incluidas:

- No entrar a las cuentas de otros usuarios
- No violar las contraseñas
- No está permitido interrumpir servicios
- No se puede compartir el acceso a las cuentas entre los usuarios

En la política de red recomendada, se determinó que exclusivamente el personal con la cuenta de administrador de red y autorizados por los Directores de cada área, está autorizado a otorgar el acceso a ciertos servicios. Es por esto que se estableció permitir el acceso desde un punto central, que otorgue sólo privilegios especiales a usuarios que les permitan llevar a cabo las tareas necesarias para hacer su trabajo. En cuanto a la creación de cuentas de usuario y la asignación de permisos, se recomiendan procedimientos específicos, para evitar confusiones y minimizar posibles errores cometidos por los administradores del sistema.

En la política de seguridad desarrollada, se definen aspectos como los derechos y responsabilidades de los usuarios y los administradores del sistema al utilizar los recursos y servicios de la red.

En cuanto al usuario:

- Restricciones en cuanto al uso de recursos
- Cuáles situaciones constituyen abuso en los términos del uso de recursos
- Política de contraseña del usuario
- Acciones legales u otro castigo a implantarse en caso de divulgar información confidencial
- Políticas de uso y acceso de cuentas
- Privacidad

En cuanto al administrador:

- Límites para revisar los directorios o archivos privados del usuario para el diagnóstico de problemas de seguridad
- Derecho de examinar el tráfico de la red

Por último, otro punto tomado en cuenta en el desarrollo de la política de seguridad, es el plan de acción cuando la política de seguridad es violada, el cual sirve para proporcionar una guía con respecto a la acción correctiva en una brecha de seguridad. Para definirla se tuvieron que ofrecer guías sobre las medidas a tomar, en base al tipo de violación del usuario de la política de seguridad en cuanto a:

- Negligencia personal.
- Accidente o error.
- Ignorancia de la política actual.
- Ignorancia deliberada de la política.

CAPITULO IV ANÁLSIS DE RIESGOS, POLÍTICAS DE SEGURIDAD Y RESULTADOS FINALES

En este capítulo se exponen los resultados obtenidos del presente trabajo, los cuales permiten mostrar alternativas de protección basadas en los requerimientos de seguridad de la organización. Las políticas de seguridad sugeridas precisan los recursos y procedimientos sujetos al nuevo ambiente de seguridad planteado y las medidas de protección presentadas son producto de la elección de las herramientas estudiadas, las cuales proporcionan la detección y clasificación de intrusos, la autenticación y control de acceso y el monitoreo permanente de la red. Los mecanismos primordiales que permitieron delinear estas políticas y medidas de resguardo, se muestran en el informe final de análisis de riesgos, el cual sintetiza los resultados obtenidos en dicho análisis.

Para realizar este análisis se utilizó la metodología de análisis de riesgos Magerit , que se orienta principalmente a evaluar los riesgos de los activos de información, los cuales son sumamente importantes ya que de esto se basó el presente trabajo para presentar las politicas de seguridad propuestas.

METODOLOGÍA DE ANÁLISIS DE RIESGO DE ACTIVOS DE INFORMACIÓN (MAGERIT)

La metodología de análisis de riesgos que se utiliza en este trabajo es la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas). Es una metodología de carácter público, la cual estudia los riesgos que soporta un sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. Esta metodología recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados. En fin, podemos definir a la Metodología MAGERIT como un método
formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse paracontrolar estos riesgos.

La estructura MAGERIT, de acuerdo a su contenido permite realizar:

- El **análisis de los riesgos** para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el Sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que secorre.
- La **gestión de los riesgos**, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

MAGERIT, como método de Análisis y Gestión de Riesgos, cubre sólo una Fase de la GESTIÓN global de la Seguridad de un Sistema de Información determinado. La Gestión global de Seguridad (Ver Fig. Nro. 13) es una acción permanente, cíclica y recurrente; es decir, se ha de reemprender continuamente debido a los cambios del sistema y de su entorno. Las otras Fases aquí sólo se enuncian y no son objeto de estudio por MAGERIT, salvo en su interfaz con la Fase de Análisis y Gestión de Riesgos.

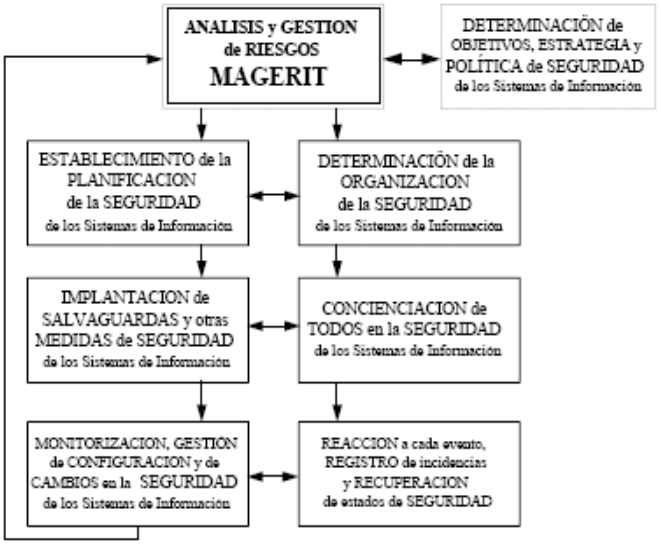

Fig. Nro. 12. Gestión Global de Seguridad

El análisis y gestión de riesgos, Fase nuclear de 'medición' y cálculo en el ciclo de gestión de la seguridad, es punto de arranque del ciclo de Gestión de Seguridad y además requiere técnicas de proceso especiales (propias del ámbito de la seguridad). Por estas causas, la Fase es objeto de un método especial, MAGERIT, mientras que las demás Fases del ciclo se apoyan en técnicas más genéricas y conocidas.

La Fase de determinación de **objetivos, estrategia y política de seguridad** de los sistemas de información se nutre de y nutre a su vez la fase de análisis y gestión de riesgos. En el ciclo inicial de la gestión de Seguridad, un análisis y gestión de riesgos de carácter global ayuda a determinar los objetivos, estrategia y política, que influirán durante los ciclos sucesivos en el análisis y gestión de riesgos más detallado (que a su vez puede modificarlos paraciclos sucesivos).

La fase de establecimiento de la **planificación** de la seguridad de los sistemas de información deriva de la fase de análisis y gestión de riesgos como su consecuencia funcional más inmediata. Utiliza técnicas generales de planificación (resultados,

secuenciación, hitos de decisión), pero adaptadas al ámbito de la seguridad.

La fase de determinación de la **organización** de la seguridad de los sistemas de información deriva de la fase de análisis y gestión de riesgos como su consecuencia orgánica más inmediata. Utiliza técnicas generales de organización (compromiso gerencial, roles, responsabilidades, documentación normativa), aunque adaptadas al ámbito de la seguridad.

La fase de **implantación de salvaguardas** y otras medidas de seguridad para los sistemas de información deriva de las fases de planificación y organización, utilizando técnicas generales de gestión de proyectos y gestión de configuración, aunque adaptadas al ámbito de la seguridad.

La fase de **concienciación** de **todos** en la **seguridad** de los sistemas de información deriva de las Fases de Planificación y Organización. Tiene en cuenta el papel fundamental del recurso humano interno en todo proyecto de seguridad y utiliza técnicas generales de Gestión de Proyectos y Gestión de Formación, Comunicación y Recursos Humanos, aunque adaptadas al ámbito de la seguridad.

La fase de **reacción** a cada evento, de **manejo y registro** de las incidencias y de **recuperación** de estados aceptables de seguridad tiene un carácter básicamente operacional y utiliza por tanto técnicas generales de gestión cotidiana y de atención a emergencias adaptadas al ámbito de la seguridad.

La Fase de **monitorización**, **gestión de configuración** y de **cambios** en la seguridad de los sistemas de información tiene un carácter básicamente de mantenimiento, con técnicas generales de monitorización, gestión de configuración y gestión de cambios adaptadas al ámbito de la seguridad.

ETAPAS DE LA METODOLOGÍA DE ANÁLISIS DE RIESGO DE ACTIVOS DE INFORMACIÓN (MAGERIT)

MAGERIT propone las cuatro Etapas siguientes:

Etapa 1. Planificación del análisis y gestión de riesgos: La etapa establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos; permite investigar la oportunidad de realizarlo; definir los objetivos que ha de cumplir y el dominio (ámbito) que abarcará; planificar los medios materiales y humanos para su realización; e iniciar el lanzamiento del proyecto.

Etapa 2. Análisis de riesgos: La etapa permite identificar y valorar los elementos que intervienen en el riesgo; obtener una evaluación de éste en las distintas áreas del dominio; y estimar los umbrales de riesgo deseables.

Etapa 3. Gestión de riesgos: La etapa permite identificar las posibles **funciones o servicios** de salvaguarda reductores del riesgo detectado; seleccionar las salvaguardas aceptables en función de las ya existentes y de las restricciones; simular diversas combinaciones; y especificar las finalmente elegidas.

Etapa 4. Selección de salvaguardas: La etapa permite seleccionar los mecanismos de salvaguarda a implantar; elaborar una orientación del plan de implantación de los mecanismos de salvaguarda elegidos; establecer los mecanismos de seguimiento para la implantación; recopilar los documentos de trabajo del proceso de análisis y gestión de riesgos; obtener los documentos finales del proyecto; y realizar las presentaciones de los resultados a los diversos niveles

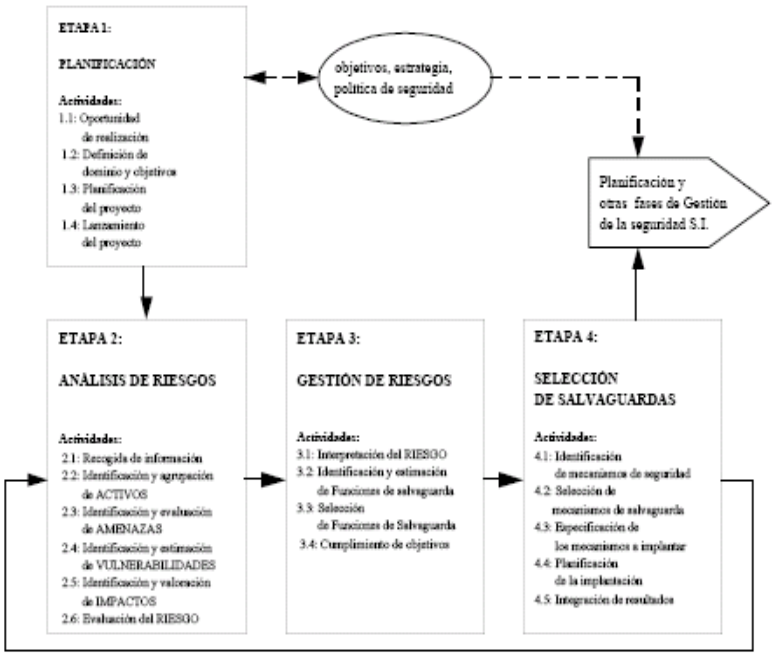

Fig. Nro. 13. Ciclo de Etapas del Proceso MAGERIT

VISION GLOBAL DE LAS ETAPAS DEL MAGERIT

La figura anterior representa el **Ciclo de Etapas (iterativo) del Proceso** cubierto por MAGERIT que constituye la fase de análisis y gestión de riesgos **dentro de la gestión de la seguridad** de los sistemas de información. Asimismo se anotan los enlaces de este ciclo MAGERIT con la fase de "Objetivos, estrategia y política de seguridad" y con la fase de "Planificación de los mecanismos de salvaguarda".

ETAPA 1. PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

Actividad 1.1: Oportunidad de realización.

Tarea 1.1.1:(única) Clarificar la oportunidad de realización.

Actividad 1.2: Definición de dominio y objetivos

Tarea 1.2.1: Especificar los objetivos del proyecto

Tarea 1.2.2: Definir el dominio y los límites del proyecto

Tarea 1.2.3: Identificar el entorno y restricciones generales

Tarea 1.2.4: Estimar dimensión, coste y retornos del proyecto

Actividad 1.3: Planificación del proyecto

Tarea 1.3.1: Evaluar cargas y planificar entrevistas

Tarea 1.3.2: Organizar a los participantes

Tarea 1.3.3: Planificar el trabajo

Actividad 1.4: Lanzamiento del proyecto

Tarea 1.4.1: Adaptar los cuestionarios

Tarea 1.4.2: Seleccionar criterios de evaluación y técnicas para el proyecto

Tarea 1.4.3: Asignar los recursos necesarios

Tarea 1.4.4: Sensibilizar (campaña informativa)

ETAPA 2. ANÁLISIS DE RIESGOS

Actividad 2.1: Recogida de información

Tarea 2.1.1: Preparar la información

Tarea 2.1.2: Realización de las entrevistas

Tarea 2.1.3: Analizar la información recogida

Actividad 2.2: Identificación y agrupación de ACTIVOS

Tarea 2.2.1: Identificar activos y grupos de activos

Tarea 2.2.2: Identificar mecanismos de salvaguarda existentes

Tarea 2.2.3: Valorar activos

Actividad 2.3: Identificación y evaluación de AMENAZAS

Tarea 2.3.1: Identificar y agrupar amenazas

Tarea 2.3.2: Establecer los árboles de fallos generados por amenazas

Actividad 2.4: Identificación y estimación de VULNERABILIDADES

Tarea 2.4.1: Identificar vulnerabilidades

Tarea 2.4.2: Estimar vulnerabilidades

Actividad 2.5: Identificación y valoración de IMPACTOS

Tarea 2.5.1: Identificar impactos

Tarea 2.5.2: Tipificar impactos

Tarea 2.5.3: Valorar impactos

Actividad 2.6: Evaluación del RIESGO

Tarea 2.6.1: Evaluar el riesgo intrínseco

Tarea 2.6.2: Analizar las funciones de salvaguarda existente

Tarea 2.6.3: Evaluar el riesgo efectivo

ETAPA 3. GESTIÓN DE RIESGOS

Actividad 3.1: Interpretación del Riesgo

Tarea 3.1.1:(única) Interpretar los riesgos

Actividad 3.2: Identificación y estimación de Funciones de salvaguarda

Tarea 3.2.1: Identificar funciones de salvaguarda

Tarea 3.2.2: Estimar la efectividad de las funciones de salvaguarda.

Actividad 3.3: Selección de Funciones de Salvaguarda

Tarea 3.3.1: Aplicar los parámetros de selección

Tarea 3.3.2: Evaluar el riesgo

Actividad 3.4: Cumplimiento de objetivos

Tarea 3.4.1 (única): Determinar el cumplimiento de los objetivos.

ETAPA 4. SELECCIÓN DE SALVAGUARDAS

Actividad 4.1: Identificación de mecanismos de salvaguarda

Tarea 4.1.1: Identificar mecanismos posibles

Tarea 4.1.2: Estudiar mecanismos implantados

Tarea 4.1.3: Incorporar restricciones

Actividad 4.2: Selección de mecanismos de salvaguarda

Tarea 4.2.1: Identificar mecanismos a implantar

Tarea 4.2.2: Evaluar el riesgo (mecanismos elegidos)

Tarea 4.2.3: Seleccionar mecanismos a implantar

Actividad 4.3 Especificación de los mecanismos a implantar

Tarea 4.3.1 (única): Especificar los mecanismos a implantar

Actividad 4.4: Planificación de la implantación

Tarea 4.4.1 Priorizar mecanismos

Tarea 4.4.2: Evaluar los recursos necesarios

Tarea 4.4.3: Elaborar cronogramas tentativos

Actividad 4.5: Integración de resultados

Tarea 4.5.1 (única): Integrar los resultados

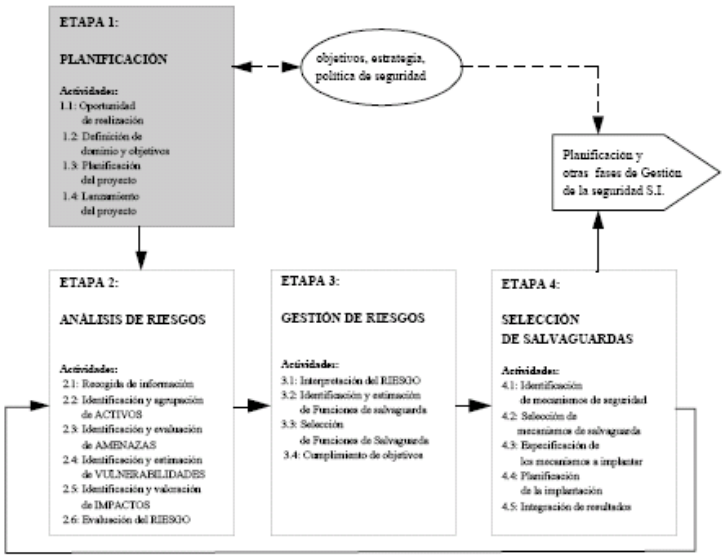

Fig. Nro. 14. Visión general del proceso MAGERIT

PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

El objetivo principal de ésta etapa es establecer y definir el marco general de referencia para todo proyecto de análisis y gestión de riesgos. Es por esto que para llevar a cabo el primer paso para la realización del análisis de riesgos de activos de información del Ministerio del Poder Popular para la Educación Superior se definieron las metas de la elaboración del mismo y de la elaboración de políticas y normas de procedimientos para la seguridad de información a largo plazo. Además de esto se estimaron las necesidades de información en función de dichas metas, tomando en cuenta la situación del Ministerio del Poder Popular para la Educación Superior, así como la visión de los responsables del mismo.

En ésta etapa se abarcaron los siguientes puntos:

- La justificación y oportunidad de abordar el proyecto.
- La definición del dominio a considerar y de los objetivos del proyecto.

- La planificación del proyecto, considerando los participantes, los recursos necesarios y el cronograma de realización.
- La particularización de las técnicas a emplear en las actividades del proyecto.

Actividades realizadas en ésta etapa:

ACTIVIDAD 1: Oportunidad de Realización: La iniciativa para la realización de un documento que contenga las adecuadas políticas de seguridad y el desarrollo de un análisis de Riesgos de activos de información para el Ministerio del Poder Popular para la Educación Superior parte de la necesidad interna de la Organización, consciente de los problemas relacionados con la seguridad de los sistemas de información, como por ejemplo, los incidentes continuados relacionados con la seguridad, inexistencia de previsiones en cuestiones relacionadas con la evaluación de necesidades y medios para alcanzar un nivel aceptable de seguridad de los sistemas de información que sea compatible con el cumplimiento correcto de la misión y funciones del Ministerio, reestructuraciones en los servicios proporcionados, cambios en la tecnología utilizada, desarrollo de nuevos Sistemas de Información, entre otros. Es por esto que, a partir de lo mencionado anteriormente, se elaboraron algunos cuestionarios-Marco (Ver anexos) donde a través de preguntas referentes a como es el manejo de los activos de información, como es el resguardo de ellos, entre otros, permitiera provocar la reflexión sobre aspectos de la seguridad de los sistemas de información por parte de Los responsables de las Unidades.

Los Cuestionarios señalados anteriormente, permitieron proceder a un examen superficial de la situación en cuanto a la seguridad de sus sistemas de información; y a través de éste los responsables de las áreas pudieron expresar su opinión por los proyectos de seguridad ya realizados, así como sus expectativas ante la elaboración de un proyecto de análisis y gestión de riesgos y el establecimiento de políticas de seguridad. Esta aproximación permitió obtener una primera visión de los objetivos concretos y las opciones políticas que tendrían que subyacer a la elaboración del proyecto de análisis y gestión de riesgos. En cuanto a los responsables del área

informática, el cuestionario permitió obtener una panorámica técnica para la elaboración del proyecto de análisis y gestión de riesgos y posibilitó abordar el estudio de oportunidad de realización del proyecto, tras integrar las opciones políticas anteriores.

Por lo anteriormente descrito y de acuerdo a los resultados obtenidos en el cuestionario-marco los directores de las unidades involucradas y la dirección de Informática estuvo de acuerdo en que se llevara a cabo la elaboración del proyecto de análisis y gestión de Riesgos, para así de acuerdo a lo obtenido.

ACTIVIDAD 2. Definición de dominio y objetivos: Esta actividad permitió determinar el alcance del proyecto y de sus objetivos, diferenciados según horizontes temporales a corto y medio plazo. Los objetivos del proyecto se especificaron en función de la finalidad de la planificación estratégica, del estado de partida de la organización y de las consideraciones de las direcciones recogidas en la actividad anterior. En ésta tarea se recopiló la documentación pertinente al Ministerio y se especificaron detalladamentelos objetivos del proyecto.

Dentro de los objetivos que se establecieron en éste proyecto se encuentran:

- Determinar las áreas de riesgo más elevado dentro del Ministerio.
- Hacer uso del análisis de gestión de riesgos para realizar una gestión integral de la seguridad de los sistemas de información.
- Desarrollo de políticas de seguridad para controlar el manejo de los activos de información.

También se identificaron en ésta actividad las unidades objeto del análisis y gestión de riesgos y se especificaron las características generales de dichas unidades en cuanto a responsables, Servicios proporcionados, etc. También se identificaron las principales relaciones de las unidades objeto del proyecto con otras entidades, por

ejemplo el intercambio de información en diversos soportes, el acceso a medios informáticos comunes, etc.

La tarea partió de un principio básico: el análisis y la gestión de riesgos la cual se centró en un dominio limitado**,** que incluyó la Coordinación de Informática y las direcciones a las cuáles ésta presta sus servicios, ya que un proyecto de ámbito demasiado amplio o indeterminado podría ser inabarcable, por excesivamente generalista o por demasiado extendido en el tiempo, con perjuicio en las estimaciones de los elementos del Análisis y Gestión de Riesgos.

Otro punto tomado en cuenta dentro de ésta actividad fue la realización de un estudio global de los sistemas de información de las unidades incluidas en el dominio del proyecto, con el objetivo de identificar sus funciones y finalidades principales y sus relaciones con el entorno, así como sus tendencias de evolución. Aquí también se identificó a las personas a entrevistar para obtener la obtención detallada de información que posibilite la Etapa 2 de Análisis de riesgos y las posibles restricciones generales que deberá tener en cuenta el proyecto.

En cuanto a las personas entrevistadas se encuentran las siguientes:

- Coordinador de Informática.
- Administrador de Redes.
- Responsable de la Unidad de Desarrollo de Sistemas de Información.
- Responsable de la Unidad de Soporte Técnico.
- Responsable de la unidad de Telecomunicaciones.

Otro de los puntos dentro de ésta actividad fue el dimensionamiento del proyecto a partir del conocimiento de los objetivos del proyecto, del dominio y del perfil de las unidades incluidas en el estudio. En función de la dimensión estimada y de los objetivos del proyecto se escogieron algunas de las técnicas a utilizar en el análisis

y gestión de riesgos. Por otra parte, también se dimensionó el proyecto en cuanto a su coste y los retornos o beneficios que pudiera aportar a futuro, para que la Coordinación de Informática tomara con fundamento la decisión de emprenderlo y asignar los recursos necesarios para su desarrollo.

El estudio del coste del proyecto se realizó sin dificultad estimando los tiempos y perfiles del personal asignado a las etapas del proyecto. El estudio de los retornos sólo puede ser muy impreciso en esta etapa inicial, pues no puede tener en cuenta aún el verdadero retorno de un proyecto de seguridad, que es precisamente el coste de no tener dicha seguridad en el dominio estudiado o sea el resultado del propio proyecto de Análisis y Gestión de Riesgos.

PLANIFICACIÓN DEL PROYECTO

Informe Final Análisis de Riesgos: Con la finalidad de evaluar la seguridad de las redes de información del Ministerio del Poder Popular para la Educación Superior, se realizó un análisis de riesgos en el Dirección de Administración y Servicios, a partir del cual se emitirá un juicio basado en sus resultados, que permitirá determinar los niveles de seguridad vigentes del Ministerio y recomendar políticas de seguridad acordes a las necesidades empresariales.

Durante la elaboración de un análisis de riesgos, se maneja información clasificada como confidencial, debido a lo delicado o importante que puede ser el contenido de la misma para garantizar la integridad de la organización, sobretodo si existen oportunidades de competencia desleal, cometer fraudes, delitos y cualquier otro tipo de amenaza que represente un riesgo para la empresa.

Esta es la razón fundamental por la que muchos de los datos que se manejaron durante este estudio no serán mencionados o serán ligeramente alterados. La siguiente información es confidencial: Toda la documentación proporcionada por el Ministerio, es considerada como confidencial y no se incluirá.

A continuación se expone el contenido de los resultados obtenidos de la realización del análisis de riesgos en las distintas áreas de la Dirección de Administración y Servicios, así como las recomendaciones que sirvieron como base para la definición de los lineamientos, enfocados hacia la posibilidad de proveer seguridad en las redes de información de la empresa.

OBJETIVO GENERAL DEL PROYECTO

Determinar las vulnerabilidades a las están expuestos los activos de información del Ministerio del Poder Popular para la Educación Superior, con la finalidad de plantear las recomendaciones necesarias para proveerlos de un nivel de protección adecuado.

OBJETIVOS ESPECÍFICOS DEL PROYECTO

- Revisar el ambiente tecnológico instalado en el M.P.P.E.S.
- Revisar los controles de rastreo y monitoreo.
- Evaluar los controles existentes para la seguridad física y lógica de los datos.

ALCANCE DEL PROYECTO

El presente análisis de riesgo evalúa los siguientes aspectos de protección de las redes de información de la institución:

- Control de Acceso.
- Integridad.
- Auditoría.
- Seguridad Física.

- Planes de Contingencias

Asi mismo, se lleva a cabo el análisis del impacto que tiene cada uno de estos aspectos en lo que respecta a la calidad (Disponibilidad, Integridad, Confidencialidad) de los activos de información que son manejados por el Ministerio del Poder Popular para la Educación Superior

LIMITACIONES DEL PROYECTO

Las limitaciones encontradas en el análisis de riesgos fueron:

- La disposición del personal que labora en el M.P.P.E.S.
- La confidencialidad de la información.
- El recelo por parte de los trabajadores a prestar colaboración al proceso de analizar los riesgos, debido al temor que causa la evaluación.
- Es la primera vez que se realiza un análisis de los riesgos de información dentro de la institución.

PLAN DE TRABAJO DEL PROYECTO

	SEMANAS								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Etapa 1: Determinación de Requerimientos de Seguridad									
Etapa 2: Analizar Activos de Información									
Etapa 3: Evaluar Riesgos									
Etapa 4: Determinar Recomendaciones									

Tabla Nro 3. Cronograma de trabajo

Recursos Físicos: Se contó con los siguientes recursos:

- Espacio Físico.
- Equipo. (Computadora portátil)

Herramientas: Las herramientas usadas fueron las siguientes:

- Revisión de manuales.
- Cuestionarios.
- Entrevistas
- Observación

Estrategias: La estrategia utilizada estaba orientada a permitir y asegurrar la calidad del trabajo realizado durante el proceso de análisis de riesgos. Se cumplieron los siguientes principios:

- Evaluar el desempeño para identificar mejoras en cada una de las áreas.
- Analizar y planear el trabajo para cubrir las expectativas.
- Mantener comunicaciones continuas con personal del Ministerio y en todas las etapas del análisis de riesgos.
- Hacer uso efectivo de la tecnología disponible.
- Administrar los trabajos para aumentar la efectividad y la eficiencia.

Durante el análisis de riesgos se siguieron los pasos indicados en MAGERIT, para verificar su efectividad. Sin embargo, no fue posible profundizar en algunos puntos ya que el Ministerior fué muy celoso en lo que a suministro de información se refería. en algunas de las áreas.

CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

El Ministerio del Poder Popular para la Educación Superior tiene y maneja diferentes tipos de información que soportan la toma de decisiones sobre sus operaciones. Esta información varía dependiendo del tipo de actividad o tarea que se efectúa en cada área específica. Para mantener la confidencialidad de la información que fue suministrada por la institución, y con la finalidad de minimizar los riesgos en esta situación, se clasificó la información de cada área evaluada, de acuerdo a los niveles establecidos en relación con la importancia e impacto que dicha información produce en el Ministerio del Poder Popular para la Educación Superior. Los resultados son los siguientes:

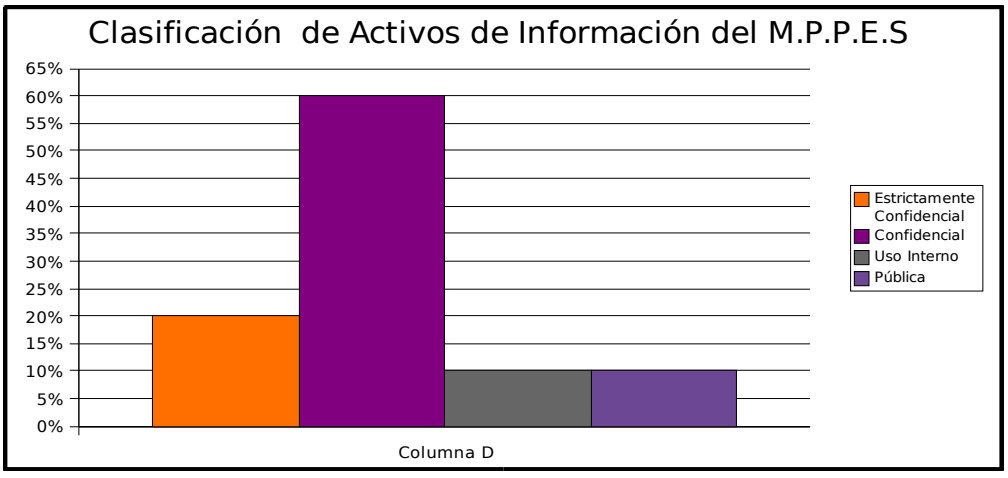

Figura Nro. 15. Distribución porcentual de la clasificación de activos de información del M.P.P.E.S

Esto indica que los activos de información de esta área, en su mayoría, son confidenciales, lo que certifica el alto impacto de la Dirección de Administración y Servicios en el desenvolvimiento continuo y eficaz de las operaciones del Ministerio del Poder Popular para la educación Superior. En conclusión, se puede afirmar que la información utilizada en esta dirección tiene las siguientes características:

- Significancia Competitiva.
- Alto grado de relevancia en la organización.
- Establece directrices.
- De gran impacto si se divulga.
- Orientada a personal autorizado o alta gerencia.

Por lo mencionado anteriormente y por la magnitud de las consecuencias que un evento contrario produciría en las operaciones diarias de la institución, se evaluó la protección de los activos de esta área para identificar los posibles riesgos a los que está expuesta y determinar las medidas de protección necesarias. Así como también establecer las prioridades en cuanto a qué activos es necesario orientar esfuerzos.

Amenazas Identificadas: Una vez identificados los activos de información que necesitan protección, se detectaron las situaciones más comunes que pueden ocasionar pérdidas a la empresa:

- Acceso no autorizado.
- Errores de Hardware.
- Errores de usuarios

Vulnerabilidades Encontradas: Después de llevar a cabo una revisión detallada de las medidas de protección vigentes en los activos de información, se identificaron las vulnerabilidades que facilitarían la ocurrencia de alguna de las amenazas. Las debilidades que se mencionan a continuación resumen el conjunto de vulnerabilidades detectadas:

- Ausencia de un Plan Estratégico de Seguridad de Información.
- Ausencia de un Departamento o personal específicamente encargado de la Seguridad de la Información.
- Deficiencia del Plan de Contingencia.

- Obsolescencia y ausencia de Documentación de Sistemas de Seguridad.
- Deficiencia en Reportes de Fallas

Luego de analizar las vulnerabilidades y amenazas identificadas se observó que el Ministerio del Poder Popular para la Educación Superior, más que requerir la implementación de medidas y controles tecnológicos, debe coordinar y establecer una estructura organizativa responsable por definir los requerimientos de seguridad de la institución y crear una conciencia en los empleados sobre la seguridad de la información ya que, aunque se establezcan mecanismos de seguridad para garantizar eficazmente la seguridad de la información administrada por la Coordinación de Informática, no se puede asegurar que no sea la concientización y educación de los usuarios la forma de mantener la seguridad de los documentos (informes, borradores, listados, etc.), generados y producidos por los usuarios contenidos en la red.

POLÍTICAS DE ADMINISTRACIÓN Y CONTROL DE SEGURIDAD

Las siguientes políticas son el resultado de la evaluación de la seguridad de la red del Ministerio del Poder Popular para la Educación Superior; están diseñadas con el fin de cubrir las necesidades y de reforzar ciertas debilidades, identificadas en el diseño de seguridad actual de la institución. Además proveen los lineamientos fundamentales que permitirán garantizar la seguridad, disponibilidad, e integridad de la información en el Ministerio, la cual abarca todos los datos e información manejadas, mantenidas y procesadas por los sistemas de la institución, hasta su transferencia segura a entes externos. Estas proporcionan un marco referencial de actuación a todos los usuarios de la red de la institución, en materia de seguridad de activos de información.

Las políticas de seguridad definen los recursos y procedimientos sujetos al nuevo ambiente de seguridad y acceso, sobre los cuales se fundamentarán los parámetros para la configuración de los mecanismos de protección. Así mismo, ayudan a preveer inconsistencias que puedan introducir riesgos, y funcionan como una base para reforzar aún más los procedimientos y reglas detalladas. Estas políticas proveen un

marco de actuación a todos los empleados del Ministerio del Poder Popular para la Educación Superior en materia de seguridad de información. No obstante, todos ellos son responsables de implementar los mecanismos de seguridad necesarios para controlar el acceso a la información que manejan. La estructura de las políticas, cuyo contenido se indica a continuación, se presenta de acuerdo a las siguientes divisiones:

En cuanto a la Organización de la Seguridad: El objetivo fundamental es establecer una estructura organizativa responsable de definir y mantener los requerimientos de seguridad de información de los usuarios de la red de la empresa. Este comité estará integrado por personal de la Gerencia de Servicios de Información, para garantizar de una manera eficiente y eficaz la protección de toda información referente a cualquier actividad de la empresa. En dicha estructura se pueden identificar tres funciones básicas; Una función principal, es la de establecer y definir los requerimientos de seguridad de cada usuario, la segunda, es la de identificar y coordinar la implantación de los mecanismos más eficientes para proveer los niveles de seguridad requeridos por los usuarios y, la tercera, es la de hacer seguimiento y dar soporte a cada una de las necesidades individuales de seguridad.

Para llevar a cabo la función de seguridad de la información, deben formarse:

- Comité de Seguridad de la Red: Representa el aspecto direccional, se encarga de formular directrices y políticas en esta materia.
- Coordinador de Seguridad de la red: Representa el aspecto técnico; llevará a cabo el monitoreo técnico de la seguridad y ejecutará las directrices del comité.
- Coordinador de Seguridad de Recursos Humanos: Representa el aspecto humano; será el responsable por el desarrollo de la cultura de seguridad en la empresa, de acuerdo con los lineamientos del mencionado comité.

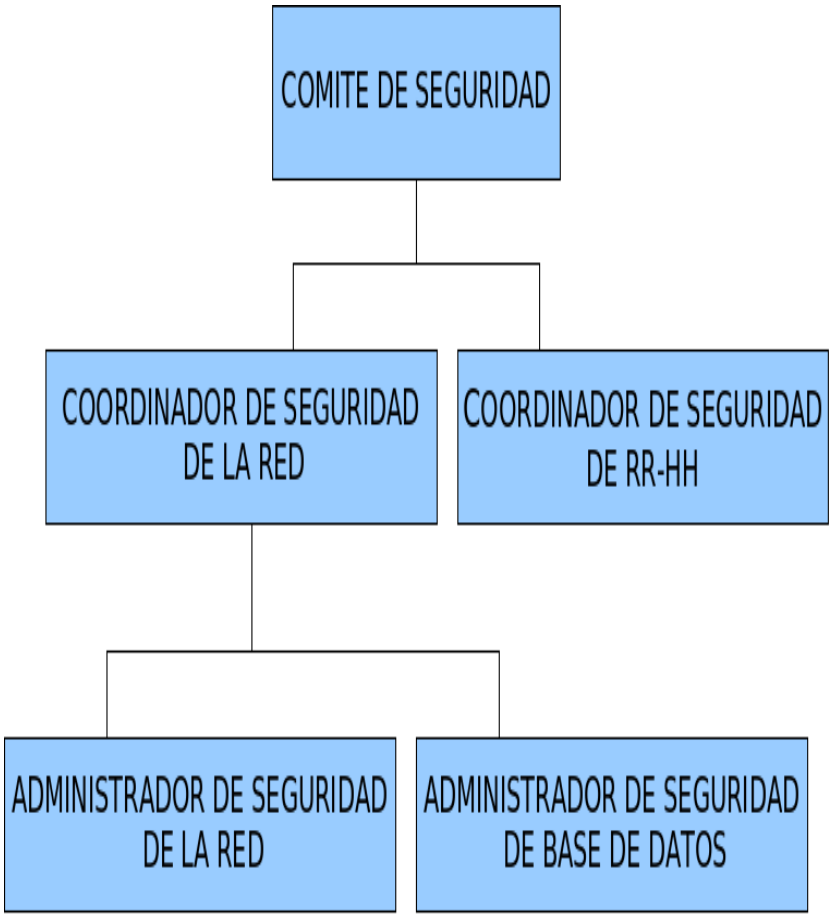

Figura Nro. 16. Estructura Organizativa para la seguridad de la información.

Cada uno de los integrantes de la estructura organizativa, así como las otras personas involucradas en el cumplimiento de los mecanismos de seguridad, deberán cumplir con unos roles de seguridad, presentados en la siguiente tabla:

ROL	DESCRIPCIÓN
Comité de Seguridad	**Figura Institucional creada para generar políticas y directrices en materia de seguridad de activos de información. El mismo estará conformado por:** • **Gerente de sistemas e informática** • **Contralor interno** • **Jefe del departamento de IT** • **Coordinador de seguridad de recursos humanos.**
Coordinador de seguridad de la red	**Este rol es ejercido por el jefe del departamento de IT, quien será responsable de desarrollar los mecanismos para llevar a cabo las políticas y directrices acordadas por el comité de seguridad.**
Coordinador de seguridad de Recursos Humanos	**Este rol es ejercido por un representante de la gerencia de recursos humanos, quien estará a cargo de diseñar y llevar a cabo programas de: inducción, educación, y/o concientización de todo el personal de la empresa, en lo relacionado con la seguridad de activos de información.**
Administrador de seguridad De bases de datos	**La función de esta figura en la organización de seguridad es la de asignar y administrar la permisología a los usuarios que utilizarán las aplicaciones que se encuentren en ambientes distribuidos en los servidores de la red corporativa.**
Dueños de información	**Es toda aquella Gerencia, Departamento, Unidad Operativa o persona responsable de generar y comunicar cualquier información dentro de los estándares establecidos.**
Custodio de la información	**Son aquellas personas, designadas por los Departamentos y/o Gerencias, que tienen la responsabilidad del resguardo físico de la información. Un mismo activo puede tener varios custodios.**
Usuario de la información	**Son todas aquellas personas autorizadas para usar la información, de acuerdo con parámetros de utilización definidos.**
Proveedor de servicios	**Entes encargados de suministrar los servicios requeridos por las unidades usuarias.**
Gerentes o funcionarios de rango similar de la alta administración	**Son aquellos funcionarios de la empresa, responsables de conocer los activos de información que manejan las unidades bajo su adscripción y de establecer los niveles de control necesarios.**

Tabla Nro. 4. Roles de Seguridad

En cuanto a Políticas Generales: El objetivo principal es proveer un marco referencial de actuación al personal de la institución en materia de seguridad de la información y dar a conocer la filosofía que en esta materia establece la misma. Estas instrucciones están dirigidas a todos los empleados del Ministerio del Poder Popular

para la Educación Superior (fijo o contratado), a los fines de incorporar las mismas en sus rutinas de trabajo.

- Todos los activos de información, manejados a través de la red del Ministerio del Poder Popular para la Educación Superior, deberán ser protegidos de manipulación, alteración, revelación, destrucción y de cualquier hecho, accidental o no, que altere la integridad de los mismos.
- Todos los empleados de la institución serán responsables de administrar la seguridad, según los lineamientos internos establecidos, y de crear los mecanismos de control de acceso a la información por ellos manejada. El personal gerencial y el área de recursos humanos son los responsables de desarrollar la conciencia de seguridad en la corporación.
- El personal gerencial de la institución será responsable de identificar y proteger todos los activos de información que están dentro del área asignada a ellos, para su control y administración, y de implantar las prácticas de seguridad en su área de adscripción.
- Todos los usuarios de la red deberán considerar las prácticas de seguridad al momento de generar los activos de información, así como también al momento de manipular los mismos, a fin de resguardarlos y garantizar su confidencialidad e integridad.
- El comité de seguridad de la red , la Coordinación de Informática y el área de Recursos Humanos, serán los responsables de desarrollar los criterios de actuación del personal en materia de seguridad, así como también de diseñar los mecanismos o procedimientos de control que garanticen la salvaguarda de los activos de información, a los fines de llevar a cabo las políticas recomendadas y poder monitorear el cumplimiento de las mismas.

En cuanto a los Usuarios de la Red: El objetivo fundamental es proveer un marco referencial de actuación a los Usuarios de la Red en materia de seguridad de la información, a los fines de incorporar las mismas en sus rutinas de trabajo.

Con el fin de no comprometer la seguridad de la red, todos los usuarios deben cumplir con las siguientes responsabilidades:

- Modificar periódicamente las claves personales de acceso a la red.
- Acatar todos los criterios y lineamientos de almacenamiento y respaldo de datos.
- Velar por el buen funcionamiento de los equipos que le sean asignados.
- Mantener respaldada y guardada, en un lugar seguro, la información que haya sido clasificada como de alto riesgo o confidencial y que se encuentre bajo su responsabilidad, así como los medios de almacenamiento, manuales y listados de información.
- Apagar el equipo una vez finalizada la jornada de trabajo.
- Destruir, previa autorización correspondiente, cualquier documento que contenga información importante y vaya a ser desechado.
- Efectuar respaldo y borrar del disco duro la información almacenada en él, cuando el área de operaciones y mantenimiento técnico deba movilizar el computador fuera de su área de adscripción, bien sea por reasignación, por reparación o cualquier otro motivo.
- Notificar de inmediato al Comité de Seguridad y la Coordinación de Informática cuando exista la sospecha o se descubra que su información ha sido manipulada sin autorización.
- No dejar información en pantallas, ni listados en la impresora, cuando deba alejarse de su puesto de trabajo.
- Realizar periódicamente pruebas de recuperación de la información respaldada.
- Informar a la Coordinación de Informática cualquier traslado, ingreso o retiro del personal o de equipos.
- Reportar al departamento de apoyo al usuario sobre cualquier

desperfecto, modificación de la configuración o instalación de programas que afecten al equipo.

- Solicitar al departamento de apoyo al usuario las reubicaciones de equipo que se consideren necesarias y esperar al personal del departamento de operaciones y mantenimiento técnico para que éste realice el traslado.
- Seguir las instrucciones emitidas por el departamento de apoyo al usuario sobre la estructura de directorios en los discos fijos.

De la protección contra virus:

- Revisar periódicamente el sistema (discos fijos, memoria RAM), con un programa antivirus aprobado por la Coordinación de Informática, para la detección de posibles virus informáticos.
- Al detectar o sospechar la existencia de virus informáticos en el equipo, reportarlo a la Coordinación de Informática.
- Revisar cualquier diskette (inclusive los diskettes originales), pen drives, o cualquier dispositivo de almacenamiento, que vaya a ser utilizados en los equipos de computación, a fin de asegurar que no contenga ningún virus informático.
- No continuar usando los equipos de computación de la institución cuando sospeche la existencia de virus informáticos y abstenerse de tomar medidas para la eliminación de los mismos.

De las prohibiciones:

Para evitar situaciones que comprometan la seguridad de la red, los usuarios no deben:

- Divulgar la clave personal de la red, que le esté asignada para el acceso a la información.
- Realizar la instalación de cualquier programa o aplicación en las

estaciones de trabajo, sin la autorización de la Coordinación de Informática.

- Instalar programas ilegales (sin licencia) en los equipos de computación de la institución.
- Acceder a la red con las claves de acceso y equipos asignados a otros usuarios sin su previa autorización.
- Trabajar en la red fuera del horario establecido.
- Comer, beber o fumar mientras esté utilizando los equipos de computación de la institución o dentro de las instalaciones de computación.
- Usar los equipos de computación de la institución para la ejecución de juegos informáticos.
- Realizar copias no autorizadas de programas instalados en su computador.
- Utilizar los equipos de computación e información de la institución para fines distintos a los cuales están destinados.
- Instalar programas o aplicaciones en los directorios de datos de los servidores.
- Extraer cualquier tipo de información de la institución sin previa autorización.

En cuanto a los Administradores de la Red: El objetivo fundamental es proveer un marco referencial de actuación a los Administradores de la Red Corporativa en materia de seguridad de la información, a los fines de incorporar las mismas en sus rutinas de trabajo.

De los Deberes: Con el fin de no comprometer la seguridad de la red, todos los administradores de red deben cumplir con las siguientes responsabilidades:

- Realizar periódicamente respaldos de la información contenida en los

directorios de datos de los servidores, con las aplicaciones seleccionadas y bajo los criterios establecidos, y realizar continuamente pruebas de recuperación de la información.

- Guardar los medios de almacenamiento y respaldo de los datos de los usuarios, manuales y listados de información en un lugar seguro, y definir un esquema de respaldo de la información así como los lugares alternativos donde se realizarán los respaldos.
- Mantener en estricto grado de confidencialidad las cuentas y las claves de acceso de los administradores y de los usuarios.
- Documentar las configuraciones de los equipos servidores, dispositivos, programas, aplicaciones, así como también cualquier cambio efectuado en las mismas.
- Mantener actualizada la bitácora con las actividades diarias de cada servidor de la red, reflejando la operación realizada y la persona responsable.
- Notificar por escrito al Coordinador de seguridad de la red, sobre cualquier cambio, problema o incidente de seguridad que ocurra en la red.
- Definir los perfiles de usuario de acuerdo con los requerimientos de éstos y asegurarse de que puedan acceder a todas las aplicaciones solicitadas y a sus datos.
- Verificar que no queden usuarios trabajando en los servidores de la red e indicar en la bitácora los usuarios, que con previa autorización, permanecerán trabajando, luego de finalizar la jornada de trabajo.
- Realizar inducción a todo el personal de la empresa acerca de las nuevas medidas adoptadas para garantizar la seguridad de activos de información.
- Asegurar que todos los programas, aplicaciones, sistemas operativos, equipos y dispositivos instalados o conectados a la red, posean funciones de seguridad acordes con los requerimientos de los usuarios.

De la Protección contra virus:

- Revisar periódicamente la memoria de los servidores de la red (discos fijos, RAM), con un programa antivirus.
- Evaluar y proponer alternativas de automatización y actualización de las facilidades para la detección y eliminación de virus informáticos de los servidores.
- Implementar mecanismos que aseguren la integridad de los datos e información de los usuarios en la red.
- Definir, diseñar, e implementar procedimientos de verificación, eliminación y recuperación de la información en caso de incidentes de virus informáticos.

De las Prohibiciones:

Para evitar situaciones que comprometan la seguridad de la red los administradores de red no deben:

- Copiar archivos de datos en los directorios de aplicaciones del servidor.
- Copiar o instalar programas o aplicaciones en los discos de datos de los usuarios del Ministerio del Poder Popular para la Educación Superior
- Facilitar la información o el acceso a ella a alguna persona, ajena o interna a la institución, que no esté autorizada para conocer o utilizar dicha información.
- Instalar o copiar programas o aplicaciones ilegales (sin licencia) en los servidores de la red.
- Acceder a la información de los usuarios almacenada en los discos de los servidores de la red.

En cuanto al nivel Supervisorio y Gerencial: El objetivo principal es proveer un marco referencial de actuación al nivel Supervisorio y Gerencial de la Red en materia de seguridad de la información, a los fines de incorporar las mismas en sus rutinas de trabajo.

- Divulgar y asesorar, a nivel de su ámbito laboral, las normas y políticas existentes sobre el uso y manejo de los recursos, desde el más alto nivel operativo, y apoyar en la concientización del personal para que actúe con conocimiento de causa en el tratamiento que debe darse a dichos recursos.
- Mantener un programa de motivación y adiestramiento para la difusión de las normas y políticas existentes relacionadas con la seguridad de la información, hardware, software y cualquier documento considerado propiedad del Ministerio del Poder Popular para la Educación Superior
- Ejecutar y hacer cumplir los procedimientos generados y aprobados para el área, los cuales regularán los aspectos relacionados con el manejo de la información.
- Velar porque el personal bajo su adscripción cumpla, en forma optima, los procedimientos y normativas establecidos para la seguridad de activos de información.
- Velar porque, al finalizar la jornada de trabajo, todos los equipos sean apagados, las estaciones de trabajo desconectadas de la red y que no quede ninguna información olvidada en lugar visible.
- Canalizar las acciones necesarias, en caso de que los trabajadores fijos, temporales o cualquier otra persona que está bajo convenio de asistencia tecnológica, infrinja las normas y políticas existentes.

En cuanto a las Medidas a tomar en caso de incumplimiento de las Políticas de Seguridad: El objetivo principal es proveer a la institución de medidas a tomar en caso de que los usuarios, sean empleados o no, violen o incumplan con las

normas, políticas y procedimientos de seguridad estipulados.

- Determinar la identidad del infractor o de los infractores.
- Determinar si el infractor es de origen interno o externo a la organización.
- Identificar si la violación ocurrió por negligencia personal, accidente o error, ignorancia de la política actual o ignorancia deliberada de la política.
- En caso de no disponer de las pruebas necesarias para inculpar al transgresor se le permitirá continuar con su conducta hasta obtener la información suficiente y así aplicar las sanciones establecidas.
- En caso de contar con las pruebas necesarias, se procederá a detener las acciones del transgresor y aplicar las sanciones establecidas.
- Los usuarios, sean empleados de la empresa o no, que violen o incumplan las normas o políticas y procedimientos establecidas serán sometidos a las sanciones administrativas contempladas por el Comité de Seguridad, la Gerencia de servicios de Información y el departamento al que pertenezca el usuario.

En cuanto a la Seguridad Lógica: El objetivo principal es mantener la operatividad de los procesos en la empresa, contemplando los aspectos relacionados con la definición y control del esquema de acceso y seguridad a los datos y las aplicaciones que se encuentren en los sistemas de computación. El mecanismo principal que debe ser tomado en cuenta es la identificación y autenticación del usuario y la validación de los derechos y privilegios de éstos sobre los recursos de la red. Este esquema de acceso debe ser definido de acuerdo a los requerimientos de información de cada usuario y las características operativas de cada unidad. La seguridad lógica contempla todo aquello que tenga que ver con la administración de usuarios (niveles de acceso, perfiles, administración de claves de acceso, etc.), así como el control de aplicaciones, entre otros.

Creación de usuarios: Cada usuario identificado en el sistema va a tener ciertas cualidades y características que van a definir sus posibilidades de acceso y utilización de los recursos disponibles en la red de la empresa. Estos permisos de acceso a la red deben ser otorgados por la estructura organizativa de seguridad, según las necesidades específicas de cada caso y tomando en cuenta lo siguiente:

- Por regla general, las aplicaciones estándares (automatización de oficinas) están disponibles para que todos los usuarios las puedan ejecutar en cualquier momento; sin embargo, existen aplicaciones especiales que sólo algunos usuarios podrán accesar. Si el usuario necesita alguna de estas aplicaciones hay que otorgarle los accesos correspondientes.
- Si el usuario solicita acceso a directorios comunes en un grupo, (una vez confirmada su autorización), según lo especificado en el grupo correspondiente, le autorizarán los derechos necesarios sobre dicho directorio. Este procedimiento se inicia cuando un trabajador de la empresa, fijo o contratado, requiera integrarse en calidad de usuario para trabajar en la Red Corporativa. Consta de los siguientes pasos, por parte del analista de red:

    - Definir el perfil del usuario y proceder a crearlo, según los requerimientos de éste.
    - Habilitar la cuenta para el acceso a la Red , asignando el usuario, al (a los) grupo(s) necesario(s), para que pueda hacer uso de los recursos que necesita.
    - Si se trata de un usuario de aplicaciones de Bases de Datos, se deberá enviar copia del reporte a la División de Base de Datos de la Coordinación de Informática, para que éste asigne las permisologías requeridas por dicho usuario para las bases de datos.

Definición de perfiles: Dependiendo de las actividades y de las operaciones que deban realizar los usuarios en la Red y para mantener la seguridad y la integridad de los datos y aplicaciones, se deben establecer perfiles de usuarios que regulen el acceso a la red y la utilización de los recursos de ésta.

Las Consideraciones Generales en este aspecto son:

- El acceso de los usuarios a los servicios de la red se hará a través del mecanismo de autenticación mediante la identificación del usuario y una clave.
- Sólo tendrán acceso a la red los usuarios a quienes les sean asignados su identificación de usuarios. Esta asignación se hará a aquellos usuarios que, dependiendo de sus actividades laborales, deben hacer uso de los servicios de red.
- Es imprescindible que todos los usuarios cuando sean definidos les sea colocado su NOMBRE COMPLETO, es decir, registrar el funcionario a quien ha sido asignado dicha cuenta de usuario y la unidad en la cual presta sus servicios.
- Sólo será permitida una clave de acceso a la red por usuario. Los únicos usuarios exentos a esta regla son los Administradores y el Supervisor, quienes, además de conocer estas claves, tendrán asignadas cuentas de usuarios ordinarios.
- Los nombres de usuarios están conformados por la primera letra del nombre y el primer apellido.
- Los nombres de usuarios definirán los derechos y privilegios que tendrán los usuarios en la red, así como los recursos y servicios que podrán utilizar.
- Los privilegios de los usuarios sobre los directorios y archivos del sistema operativo y de las aplicaciones deberán ser mínimos para evitar

que éstos puedan modificar o borrar algún archivo; sólo tendrán acceso a los directorios de sistemas de las aplicaciones existentes en los servidores para lectura y así poder ejecutar las aplicaciones.

- Una vez realizado con éxito el proceso de entrada a la red, el usuario deberá ser ubicado automáticamente en su directorio de trabajo, en el cual se encontrarán todos sus archivos de datos personales.
- Para los usuarios que no tengan equipo asignado, éstos podrán hacer uso de cualquiera de los equipos de su unidad, pero respetando el número máximo de conexiones simultáneas a la red permitidas por usuario que es de una (1). De esta forma, ninguna clave podrá estar activa desde dos lugares distintos al mismo tiempo.
- Debe existir un directorio público, sobre el cual todos los usuarios tienen todos los derechos y donde estos usuarios podrán colocar archivos de datos que deseen compartir con otros usuarios.
- Los Administradores serán responsables de cualquier situación ocurrida que tuviese relación con el área a la que estén asignados.

Definición de Grupos de Usuarios: La definición de grupos de usuarios se hará de acuerdo a las unidades operativas de la institución y a las aplicaciones que se instalen en la red, tomando en cuenta los siguientes aspectos:

- Existirá un grupo por cada dirección de la institución, a la cuál pertenecerán todos los empleados de dicho dirección. Con la asignación de los usuarios a esos grupos se permitirán servicios comunes y la posibilidad de compartir datos entre ellos.
- Para las funciones de administración de los sistemas operativos, manejadores de bases de datos y las aplicaciones, existirán grupos definidos por cada una de las funciones asociadas. Estos grupos poseerán características y derechos para permitir a sus miembros la realización de las tareas asociadas con sus

funciones.

- A medida que sean incorporadas más aplicaciones a la red, éstas deben ser definidas para los usuarios y los grupos para las cuales estén destinadas.
- Para cada aplicación de bases de datos existirá un grupo definido con los atributos y derechos sobre directorios necesarios para poder accesar dicha aplicación, desde el punto de vista del sistema operativa.

Cada usuario perteneciente a un grupo, dependiendo de sus características puede tener distintos niveles de seguridad sobre las aplicaciones, acceso a red y entorno gráfico. Con la finalidad de mantener un estándar se procederá a clasificarlos en:

Grupo Básico: es el grupo que tiene el mayor nivel de restricción en cuanto a uso de aplicaciones, acceso a red y entorno gráfico. Este grupo existe para todos aquellos usuarios con una interface gráfica tipo Windows. Deben cumplir con las siguientes restricciones:

En referencia al panel de control, el usuario no podrá accesar a:

- El panel de control de pantalla; por lo tanto, no podrá modificar la apariencia, fondo y protectores de pantalla.
- El panel de control del sistema; por lo tanto, no podrá modificar la configuración de identificación y control de acceso.
- El panel de control del sistema; por lo tanto, no podrá modificar la configuración de administración de dispositivos, perfiles de hardware, el sistema de archivo y memoria virtual.

En referencia al ambiente de escritorio, el usuario no podrá cambiar:

- La configuración del papel tapiz, el cual será estándar.

En referencia a la red, el usuario no podrá cambiar:

- La configuración de la red para compartir archivos e impresoras
- En referencia al ambiente genérico, el usuario no podrá:
-
- Tener más de una carpeta de programas para las aplicaciones de automatización de oficina estándar.
- Ejecutar programas distintos a los que se ha dado acceso.
- Modificar la configuración del ambiente genérico.
- Tener acceso al entorno de red del sistema operativo.

En referencia al sistema, el usuario no podrá:

- Tener acceso a las herramientas de modificación de configuración del sistema operativo.
- Tener acceso al ambiente nativo del sistema operativo MS-DOS.
- Ejecutar aplicaciones para MS-DOS.

Grupo Especial: es el grupo que incluye a todos aquellos usuarios que necesitan mayor libertad para trabajar en un ambiente gráfico tipo Windows o Linux. Deben cumplir con las siguientes restricciones:

En referencia al panel de control, el usuario no podrá accesar:

- El panel de control de la clave de acceso; por lo tanto, no podrá modificar la configuración de su clave secreta, administración remota y perfiles de usuarios.
- El panel de control del sistema; por lo tanto, no podrá modificar la configuración de la administración de dispositivos, perfiles de hardware, el sistema de archivos y memoria virtual.

En referencia al ambiente de escritorio, el usuario no podrá cambiar:

- La configuración de la red para compartir impresoras

En referencia a la red, el usuario no podrá cambiar:

- La configuración de la red para compartir impresoras

En referencia al ambiente genérico, el usuario no podrá:

- Tener más de una carpeta de programas para las aplicaciones de automatización de oficina estándar.
- Ejecutar programas distintos a los que se ha dado acceso.
- Modificar la configuración del ambiente genérico.
- Tener acceso al entorno de red del sistema operativo.

En referencia al sistema, el usuario no podrá:

- Tener acceso a las herramientas de modificación de configuración del sistema operativo.
- Tener acceso al ambiente nativo del sistema operativo MS-DOS.
- Ejecutar aplicaciones para MS-DOS.

Grupo Supervisor: tiene acceso a modificar la configuración de su estación de trabajo, además de tener todos los derechos de instalar aplicaciones y modificar el entorno de red. Estos accesos están dados sobre todas las herramientas y paneles de control que posee un ambiente gráfico tipo Windows o Linux.

Definición de usuarios:

- La permisología de cada uno de los usuarios se realizará mediante la asignación de los usuarios a los grupos correspondientes, evitando así la asignación individual de derechos a cada uno de los usuarios.
- Existirá un usuario Administrador del Manejador de Bases de Datos para cada servidor de la institución. Este usuario será el encargado de administrar los parámetros del manejador de base de datos asociados con el sistema operativo del servidor.
- Existirá un usuario Administrador de Bases de datos por cada aplicación instalada en el servidor. Este usuario estará encargado de otorgar las permisologías a los usuarios para accesar a las bases de datos asociadas con la aplicación.

Restricciones por defecto para los usuarios

- Las cuentas de usuario regular de la red no tendrán fecha de expiración.
- El número de conexiones concurrentes será limitado y el número máximo de conexiones concurrentes permitidas seráde una (1).
- Para cada usuario nuevo que sea definido deberá crearse un directorio raíz, donde el usuario podrá colocar sus datos personales.
- Es obligatorio que todo usuario en la red tenga asignado una clave como medida de seguridad para el acceso a la red.
- Es obligatorio el cambio periódico de las claves.
- Se permitirán sólo tres (3) intentos no exitosos de conexión a la red.
- El cambio periódico de los password de los usuarios deberá hacerse por claves únicas. Esto quiere decir que cuando un usuario debe cambiar su clave, no podrá usar las anteriormente empleadas.

RECOMENDACIONES PARA LOS USUARIOS REFERENTES A PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

La siguiente lista contiene prácticas que aumentan el riesgo de la introducción de virus en la red y las estaciones de trabajo; por lo tanto, no deben llevarse a cabo. La mayoría de los puntos descritos sólo son posibles en máquinas con diskette.

1. Usar diskettes de origen desconocido en las estaciones de trabajo.
2. Intercambiar programas de aplicaciones con personas extrañas o con personas que intercambian programas frecuentemente.
3. Ejecutar cualquier programa si no se está seguro de: su origen, número de veces que ha sido copiado, si ha sido alterado.
4. Ejecutar cualquier programa de aplicación por primera vez, sin antes haber realizado respaldo de los datos y las aplicaciones en disco.
5. Llamar a otras computadoras usando módem telefónico.
6. Inicializar el sistema desde una unidad de diskette.
7. Permitir a alguna persona usar y colocar diskettes en la estación de trabajo.
8. Usar copias de sistemas operativos o programas de aplicaciones no autorizados.

Para la recuperación de archivos infectados con virus, sólo deberán ser usados respaldos que hayan sido verificados con los programas antivirus utilizados por la empresa. Es importante que, después de haber realizado la limpieza de los servidores y estaciones de trabajo luego de la infección de un virus, se mantenga un período de cuarentena en el cual los controles y verificación de existencia de virus sean más intensos.

En cuanto a los Servicios de Red: El objetivo principal es asegurar que los

usuarios que se conecten a través de algún servicio de la red, utilicen adecuadamente éstos de acuerdo a las restricciones establecidas. Se debe procurar reducir al mínimo los servicios que no sean necesarios en la red y documentar la política implementada por servicio, así como el manejo de casos no estándares. Los servicios que se encuentran activos en la red son:

Correo Electrónico

- El usuario deberá cerrar su sesión de este servicio al ausentarse de su puesto de trabajo.
- Toda información contenida en el correo electrónico del usuario será de su responsabilidad.
- Queda prohibida la activación de más de una sesión de este servicio por usuario o código.
- El administrador del servicio debe mantener activas las políticas de número de caracteres en la contraseña estándar, no utilización de las últimas cinco (5), expiración a los 30 días y duración mínima de un (1) día.

Acceso Remoto

- Toda conexión vía acceso remoto a las redes de la institución debe ser realizada a través de servidores de acceso remoto, destinados para tal fin.
- Es responsabilidad del usuario la protección de la información y divulgación de la misma, que pudiese obtener a través de una sesión de acceso remoto.
- Los usuarios de acceso remoto sólo estarán autorizados para efectuar una sóla sesión, a la vez, de conexión remota a las redes de la institución.

- Es responsabilidad del usuario mantener actualizados los mecanismo de protección instalado en cualquier equipo donde esté trabajando.
- Los usuarios que se conecten a través de este servicio no deben instalar y/o copiar ningún software en los servidores o estaciones de trabajo de la empresa, a menos que estén expresamente autorizados.
- Los usuarios no deberán utilizar sistemas con información confidencial a través de este servicio, a menos que estén autorizados.
- El administrador servicio debe garantizar que el usuario será notificado al momento de conectarse cuándo fue su última conexión.
- Para efectos de auditoría, se debe identificar cada uno de los usuarios del acceso remoto, así como el puerto desde donde realizó dicha conexión.
- Toda comunicación en línea deberá ser autenticada por algún mecanismo que lo permita, antes de conectarse a cualquier red de la institución.
- El administrador o suplidor de servicio monitoreará periódicamente las auditorías activadas en el servidor respectivo.

Internet

- Toda conexión hacia este servicio debe efectuarse a través de los firewalls o cortafuegos disponibles para tal fin; por lo tanto, las conexiones por modems o tarjetas similares quedan prohibidas, a menos que estén expresamente autorizadas.
- Cuando se efectúen servicios de FTP (File Transfer Protocol) los archivos bajados deben ser pasados por procesos de antivirus antes de ser uitlizados.
- Está totalmente prohibido bajar o consultar información e imágenes pornográficas.
- No deberá enviarse información confidencial hacia Internet a través

de las redes de la empresa, a menos que esté expresamente autorizado y protegido con los servicios exigidos de seguridad.

- El administrador o suplidor del servicio debe garantizar la implantación de mecanismos de encriptación para información confidencial que se envíe hacia Internet.
- Se debe impedir que las direcciones IP (sólo alias o sobrenombres), protocolos (sólo traducción) y contraseñas o password (reusables) transiten a través del firewall.

En cuanto a la Seguridad Física: El Objetivo principal es asegurar que únicamente el personal autorizado tenga acceso a las áreas donde se encuentran ubicados los equipos de procesamiento y transmisión de datos, así como también vigilar que el ambiente de seguridad donde se encuentren ubicados los datos sea lo más adecuado y seguro posible. La seguridad física debe ser implementada eficientemente para reducir el riesgo resultante del acceso no autorizado a los equipos de procesamiento y transmisión de datos. Unicamente debe ser permitido el acceso a personal autorizado y todo acceso de visitantes debe ser aprobado por el Coordinador de Seguridad y monitoreado por elAdministrador de ella.

Los procesos relacionados con la seguridad física de las instalaciones de procesamiento de datos son:

Identificación de personal

- Sólo tendrá acceso a las áreas restringidas el personal encargado de la administración de seguridad de la red.
- El control de acceso físico a los centros de computación donde se encuentran los equipos de la red lo ejercerá la Coordinación de Informática, otorgando acceso a aquellas personas que lo requieran para realizar sus funciones.
- Los visitantes que entren en contacto con los equipos de

procesamiento y transmisión de datos de la red, deben estar debidamente autorizados y supervisados por parte de la Administración de la Red.

- Se consideran áreas restringidas: Cuartos de cableado de la red, Salas de servidores y cualquier lugar donde se encuentren dispositivos de red.
- Sólo tendrán acceso a áreas restringidas aquellas personas que para cumplir sus funciones requieran entrar a ellas.

Controles de planta física

- El control de la planta física donde se encuentran instalados los equipos de la red debe llevarse de la manera más estricta posible.
- La mayoría de los equipos de computación y de telecomunicaciones deben encontrarse en un ambiente con condiciones óptimas de temperatura, humedad y polvo para garantizar el buen funcionamiento y prolongar el tiempo de vida útil de los mismos.
- Es recomendable que cualquier equipo que se instale sea colocado en el centro de cómputo debido a que en éste ya se han dispuesto controles ambientales de comprobada funcionalidad.
- Cualquier lugar donde vayan a ser instalados equipos para la red, debe ser acondicionado para garantizar el buen funcionamiento de los equipos y minimizar el riesgo de fallas que afecten a los usuarios y los servicios de la red.
- Debe mantenerse un inventario de los equipos de computación para llevar un control de los equipos y dispositivos que están siendo destinados a los servicios de la red.
- Debe mantenerse un inventario estricto del software y el número de licencias legales y disponibles en los servicios de la red para evitar problemas legales en contra de la institución.

- Es recomendable conectar cada servidor a una unidad de suministro de electricidad ininterrumpida (Uninterruptible Power Supply UPS), para proveer energía de respaldo si el suministro comercial falla.
- Es recomendable usar protección eléctrica para las estaciones de trabajo y para los dispositivos de interconexión de la red.

MEDIDAS DE PROTECCIÓN TECNOLOGICAS

El propósito de adoptar medidas de seguridad en redes es proteger la red privada de la institución contra intrusos, prevenir el uso no autorizado de los sistemas y proteger la información de los propietarios del Ministerio del Poder Popular para la Educación Superior. Esto se resume en el diseño de una política de seguridad, que refleje los resultados de la evaluación de la seguridad de la red y esté complementada por la selección de herramientas que ayuden a mantener la inviolabilidad de la misma. Para seleccionar estas herramientas es necesario establecer los requerimientos de seguridad de la red a proteger y luego realizar su configuración en base a las políticas de seguridad establecidas.

En cuanto a Autenticación y control de acceso: Entre los aspectos que proporciona el firewall, se encuentra la autenticación y control de acceso, a través del establecimiento de reglas, tanto de origen como de destino, que permiten comprobar el acceso a la red. Estas reglas deben ser especificadas en orden de precedencia, de las más restrictivas a las generales, y expresamente permitir el acceso, ya que, de lo contrario, todo el acceso será negado. Para este fin, el perímetro del firewall debe ser definido, especificando de quién y dequé la red debe ser protegida.

El acceso a los servicios se puede restringir basándose en:

1. Nombres de Usuarios.

2. Origen/Destino .

Nombres de usuarios: El proceso de autenticación puede ser diseñado para actuar sobre grupos de servicios, en los cuales se especifica que para disponer de ese servicio es necesario ser un usuario autorizado. Para utilizar las reglas de restricción de usuarios es necesario crear user ID, en la base de datos interna del firewall, creada para la autenticación de nombres de usuarios. Esta base de datos mantiene un registro para cada usuario, incluyendo el mecanismo de autenticación que se utiliza para cada uno de ellos y el tipo de protocolo de autenticación que va a ser aplicado a dicho usuario.

A su vez, también se establece el status de autenticación del usuario, que puede ser:

- Habilitado cuando el usuario puede accesar el firewall repetidas veces.
- Habilitado una sola vez cuando el usuario puede accesar el firewall una vez.
- Deshabilitado cuando el usuario no puede accesar el firewall.
- Temporalmente deshabilitado cuando por cierto período de tiempo no puede accesar al firewall.

Origen/Destino: La autenticación también puede ser realizada a través del establecimiento de reglas de permiso, por cada servicio, que reflejen exactamente el modelo de seguridad que se ha diseñado, como por ejemplo:

1. Direcciones origen.
2. Direcciones destino.
3. Usuarios.
4. Si requiere autenticación para poder ser utilizado

Cuando se utiliza un firewall de filtrado de paquetes, la autenticación y control de acceso no es posible, ya que ésta se realiza a través de las aplicaciones mediante los proxys.

En cuanto a Mecanismos de Detección y Clasificación: El firewall por medio de la verificación de los controles de acceso, establecidos en la configuración de cada uno de los proxys de aplicaciones de los servicios, provee reportes detallados del tráfico que circula entre las redes y hace un seguimiento exhaustivo de la información que circula a través de él, para facilitar al administrador de la red la detección y clasificación de intrusos.

Para este fin, es necesario especificar quiénes pueden acceder a los servicios de la red y qué servicios están disponibles según los requerimientos de la empresa. Estas especificaciones están documentadas en las políticas de administración y control de la seguridad en la sección anterior.

Los reportes detallados de seguridad, para detectar y clasificar los usuarios, proveen información de los servicios que están en uso y de la configuración actual del firewall referentes a:

1. Usuarios autorizados a utilizar los servicios.
2. Usuarios que envían mensajes y la fecha de emisión.
3. Usuarios que hicieron login.
4. Usuarios a los cuales se les negó algún servicio.
5. Servicios que fueron negados.

Estos reportes pueden ser emitidos diariamente, brindando una estadística del tráfico y el uso de los registros de ese día, o semanales, mostrando un resumen del tráfico manejado durante la semana. Pueden ser ejecutados con la frecuencia que se requieran y su salida es enviada automáticamente al administrador del firewall por medio de correo electrónico.

También el firewall cuenta con el sistema de registros, el cual contribuye a la detección y clasificación de intrusos, permitiendo establecer una expresión regular en el

archivo de configuración e invocando programas específicos cuando un registro de entrada cualquiera es recibido. Esto permite al administrador provocar la suspensión de un proceso o dirigir un mensaje de alerta cuando un evento adverso ha sido detectado.

Estos sistemas de registro son almacenados una vez a la semana y después de 14 días pasan a un formato comprimido de almacenamiento. El sistema de registro puede ser utilizado como un mecanismo primario de alerta, que indique al administrador la existencia de problemas de configuración, errores en el sistema o condiciones de peligro.

Otro mecanismo de detección de intrusos es el sistema de alarma, que permite alertar al administrador de problemas potenciales que puedan existir. Periódicamente, el sistema de alarma ejecuta un chequeo de la información que ha sido accesada al sistema de registro. En este sistema se define una lista de los sucesos que no son importantes para que sean ignorados, mientras que todo otro suceso es traído al administrador del sistema para su atención. El sistema de alerta es chequeado constantemente y cualquier salida generada por él es enviada electrónicamente al administrador del firewall inmediatamente.

Los resultados de esta investigación pretenden sentar las bases para guiar la implementación de la "tecnología" de seguridad, la cual tiene como finalidad establecer la dependencia entre las políticas de seguridad sugeridas y las medidas de protección tecnológicas seleccionadas. Logrando así unificar esfuerzos que permitirán elevar el nivel de seguridad actual.

RECOMENDACIONES

Una vez definidos los riesgos a los que está expuesta la información, delimitado el espacio a abarcar y el espectro de posibles soluciones de cada una de las necesidades específicas, se presentan una serie de recomendaciones enfocadas hacia la posibilidad de proveer seguridad y privacidad individual a la información almacenada en los sistemas automatizados de la Dirección de Administración y Servicios. Estas recomendaciones proveen las bases para la definición de lineamientos para la seguridad de la información. En forma general, los objetivos son los siguientes:

- Establecer una estructura organizativa responsable por definir y mantener los requerimientos de seguridad de la información.

- Formular, documentar y distribuir las políticas, normas y procedimientos en materia de seguridad.

- Evaluar continuamente las políticas, normas y procedimientos de seguridad para, eventualmente, introducir cambios y mejoras necesarias.

- Establecer mecanismos de control para la seguridad de la información en la red.

- Desarrollar políticas escritas sobre la privacidad, describiendo por qué, cómo y qué sobre la recolección de información por la institución.

- Diseñar el procedimiento para asignar las autorizaciones en el sistema y definir los perfiles de los usuarios, de manera que se garantice que las autorizaciones establecidas sean las que el usuario requiere.

- Formular políticas escritas sobre la propiedad de los archivos de datos, escribiendo claramente las responsabilidades de los dueños y usuarios.

- Formular e implementar un compromiso de confidencialidad de información, por parte de los usuarios.

- Definir la función de Auditoría de Seguridad de Información y sus responsabilidades.

- Definir funciones, procedimientos, responsabilidades y permisología de acceso referente a la seguridad de activos de información, dependiendo de las funciones del empleado.

- Establecer medidas disciplinarias a ser tomadas en caso de detectar fraude, hurto o destrucción, modificación o revelación de la información de la institución

- Definir claramente las limitaciones de los empleados para hacer uso de los recursos de procesamiento de información de la empresa.

- Establecer y formalizar los procedimientos para controlar las modificaciones al sistema operativo y programas de aplicaciones de cada estación de trabajo.

- Formalizar un proceso de documentación que controle el registro de las fallas ocurridas y la descripción de una solución.

- Formalizar, difundir e implementar una política de control de respaldos y recuperaciones.

- Incrementar los niveles de seguridad de la confidencialidad de las claves, restringiendo el acceso a los archivos que contienen la clave secreta de los usuarios, sólo a los niveles supervisiorios responsables del área de sistemas.

- Establecer controles que garanticen la continuidad de los servicios de informática.

- Establecer mecanismos que permitan la detección y/o eliminación de virus, lo cual puede evitar la pérdida de información vital en la institución.

- Realizar un monitoreo de la red que permita atribuir, de forma veráz, la responsabilidad, al detectarse un procedimiento fraudulento en los activos informáticos.

- Programar, con prioridad, la formalización de un plan de contingencia, debidamente documentado, revisado, actualizado y probado por lo menos una vez al año, con el fin de garantizar la continuidad de las operaciones, en caso de desastres.

- Registrar y realizar un seguimiento formal de fallas para controlar la efectividad de las aplicaciones, así como también conocer los resultados que arrojan para medir y establecer estadísticas sobre las interrupciones generadas y diseñar un plan de mantenimiento efectivo que permita erradicar las mismas.

- Planificar, diseñar y ejecutar planes de educación para los empleados del Ministerio del Poder Popular para la Educación Superior lo cual puede comprender: organizar charlas, conferencias, cursos, programa de inducción y folletos educativos.

- Diseñar y establecer procedimientos para la destrucción de la información confidencial cuando ésta deba ser desechada, a fin de evitar la fuga de la misma a personas no autorizadas.

CONCLUSIONES

Debido a los grandes cambios tecnológicos que se han venido aconteciendo con el pasar del tiempo, las organizaciones se han dado cuenta que dependen en gran parte de su infraestructura tecnológica. Por lo tanto, las organizaciones e instituciones tanto públicas como privadas deben responsabilizarse por garantizar la seguridad, integridad y confidencialidad de la información que es manejada por ellos. Hay que considerar que este manejo constituye un punto importante para el desarrollo de las operaciones organizacionales, y es por esto que es sumamente necesario el establecimiento de controles de seguridad para la protección y prevención de sus activos de información.

Es de vital importancia tener en cuenta que la alta gerencia debe tomar conciencia sobre la realización de un análisis de riesgos de sus activos cada cierto tiempo, y poner en práctica métodos más efectivos para protegerlos contra ataques y fallos provocados o no provocados, para alcanzar los objetivos operacionales de una forma efectiva y eficiente.

Es importante señalar que en este trabajo de grado se diseña una metodología para establecer las políticas de seguridad de información adecuadas para el Ministerio del Poder Popular para la Educación Superior las cuales servirán para resguardar sus activos de información ante cualquier riesgo que se pueda presentar. Una vez lista la metodología el siguiente paso será la implementación de dichas políticas de seguridad de información, en donde la puesta en marcha de las mismas estará a cargo del Ministerio del Poder Popular para la Educación Superior.

Por otro lado se logró no solo el establecimiento de políticas de seguridad de información para este Ministerio, sino que además este documento pudiera ser la base para el establecimiento de controles y medidas de seguridad de información, que pudieran servir como guía, para cualquier institución tanto pública como privada, ya que como se menciona dentro de este documento, la guía para llevar a cabo el mismo fueron estándares internacionales y la metodología de análisis de riesgos seleccionada

fue la que más se adaptaba a las necesidades de la institución, sin embargo se mencionan otras metodologías que pudieran servir como herramientas para que cualquier organización pueda determinar la situación de sus activos de información y tome las previsiones al respecto de acuerdo al resultado del análisis realizado.

El punto más importante de considerar antes de poner en prácticas políticas de seguridad de algún tipo, debe ser un estudio detallado de los riesgos a los que se encuentra expuesta la información, los servicios y el equipamiento de red. Este punto quizas no es muy tomado en cuenta, lo cual conlleva a un gran error, ya que es necesario delimitar el espacio a abarcar por el plan y el espectro de posibles soluciones a cada una de las necesidades específicas. Además de esto, se deben considerar el nivel de importancia de las aplicaciones, datos o servicios y el tipo de usuarios que las utilizan, ya que son dependientes del tamaño y la naturaleza de las operaciones realizadas por los sistemas automatizados en la empresa. Es necesario destacar además que, aunque se pueden establecer mecanismos para garantizar la seguridad de la información a través de herramientas tecnológicas, no se puede asegurar, que con la implantación de éstas el problema sea resuelto, ya que, luego de analizar los principales riesgos a los que está expuesta la información, se puede afirmar que la mayoría de los problemas, en el área de tecnología en general, son ocasionados por la conducta de los empleados quienes no hacen uso adecuado de los activos de información de las organizaciones.

REFERENCIAS BIBLIOGRÁFICAS

Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC). La Gestión de la Seguridad de la Información.

Bellovin, S., Cheswick, W., Gosling, J. y Ford, W. (1998, Octubre). How security Computer Works. Scientific American. Pp. 106-109.

Cavedatos. Políticas de Seguridad Informática. Mejores Prácticas. Disponible en: www.cavedatos.org.ve/download/cdt_289.pps

Dalton, G., (1998, agosto 31). Acceptable Risks. InformationWeek. [Online]. Pp.1-6.

Denning, D. (1999, Abril). Who's Stealing Your Information?.Infosecurity.

Farley, M., Hsu J. y Stearms, T. (1997) Guía de Seguridad e Integridad de Datos. Disponible en: http://www.delitosinformaticos.com/articubs/100530260583540.shtml

Jeimy Cano Martínez. (2000). Pautas y recomendaciones para elaborar políticas de seguridad informática. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m142a.htm

Magazine.[Online].Pp.1-6.Disponible:http://www.infosecuritymag.com/apr99/cover.htm [1999, Junio 4].

Ministerio de Administraciones Públicas. (2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Catálogo de elementos. Madrid, España.

Disponible en: http://www.csi.map.es/csi/pdf/magerit_v2/catalogo_v11_final.pdf

Ministerio de Administraciones Públicas. (2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía de Técnicas. Madrid, España.

Disponible en: http://www.csi.map.es/csi/pdf/magerit_v2/tecnicas_v11_final.pdf

Ministerio de Administraciones Públicas. (2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Método. Madrid, España.

Disponible en: http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

Oficina Nacional de Tecnologías de la Información (2005). Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. Documento Público. Argentina.

Stalling, William. 1998. Cryptography and Network Security: Principles and Practice, 2/e. Prentice Hall.

Tanembaum, A. (2003). Redes de computadores. (4a ed.).(p. 754) Pearson - Prentice Hall.

Universidad Nacional de Colombia. (2003). Guía para la elaboración de Políticas de Seguridad. Disponible en:

www.unal.edu.co/seguridad/documentos/guia_para_elaborar_pditicas_v1_0.pdf

UPEL. (2003) Manual de Trabajos de Grado de Especialización y Maestria y Tesis Doctorales. Impreso por Fidetel, Caracas.

A N E X O S

Políticas de Seguridad															
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Política de seguridad	**Documento de Política de Seguridad de la Información**	¿Existe un documento de política de seguridad disponible para todos los usuarios?		**x**								**x**	**x**	
	Revisión y evaluación	¿Se hacen revisiones regulares de la política de seguridad?		**x**								**x**	**x**	

Anexo Nro 1. Cuestionario Políticas de Seguridad

Organización de la Seguridad de Información															
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Infraestructura de seguridad	**Comité de Seguridad de la Información**	¿Existe un comité de seguridad que trate las cuestiones de seguridad?		**x**									**x**	
	Coordinación de la Seguridad de la Información	¿Se coordinan las medidas de seguridad entre los distintos departamentos?		**x**								**x**	**x**	
	Asignación de responsabilidad sobre Seguridad de la Información	¿Están definidas las responsabilidades para proteger y controlar la información y los sistemas?	**x**											
	Proceso de autorización de recursos para el tratamiento de la información	¿Existe un proceso de autorización de la dirección para instalar nuevos equipos o aplicaciones?	**x**											
	Asesoramiento de especialistas en seguridad de la información	¿Cuenta su empresa con el asesoramiento de un especialista en seguridad?		**x**									**x**	**x**
	Cooperación entre Organizaciones	¿Mantiene su empresa contactos con organizaciones especialistas de seguridad?		**x**									**x**	**x**
	Revisión Independiente de la Seguridad de la Información	¿Se realizan revisiones independientes de la implantación de la seguridad?	**x**											

Seguridad en el acceso de terceros	**Identificación de riesgos por el acceso de terceros**	¿Se han identificado los tipos de acceso y los motivos por lo que terceros puedan acceder a los sistemas o la información de la empresa?	**x**												
	Requerimientos de Seguridad en contratos con terceros	¿Se ha valorado e incluido en el contrato con terceros los aspectos relacionados con la seguridad de la información?		**x**											**x**
Subcontratación	**Requerimientos de seguridad en contratos de Externalización**	¿Están definidos en los contratos de subcontratación los requisitos de seguridad de la organización subcontratante?		**x**											**x**

Anexo Nro. 2 Cuestionario Organización de la Seguridad de Información

Gestión de Activos															
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Responsabilidad de los activos	**Inventario de activos**	¿Existe un inventario actualizado de los activos del sistema de información?	**x**											
Clasificación de la información	**Guías de clasificación**	¿Existe un esquema para clasificar la información y los sistemas en función de su confidencialidad o importancia?		**x**							**x**		**x**	
	Marcado y tratamiento de la información	¿Existen procedimientos para identificar y usar la información, según su clasificación?		**x**							**x**		**x**	

Anexo Nro 3. Cuestionario Gestión de Activos

Seguridad Recursos Humanos																
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Definición del puesto de trabajo	**Inclusión de la seguridad en las responsabilidades laborales**	¿Están documentadas las funciones y responsabilidades de los puestos de trabajo?		**x**					**x**		**x**			
	Selección y política de personal	¿Se verifica que son ciertos los datos del CV cuando se solicita un puesto de trabajo?		**x**										**x**
	Acuerdos de confidencialidad	¿Firman los empleados un acuerdo de confidencialidad?		**x**							**x**		**x**	
	Términos y condiciones de la relación laboral	¿Están establecidas las responsabilidades de los empleados, relativas a la seguridad, en los términos y condiciones del contrato de trabajo?		**x**									**x**	
Formación de los usuarios	**Educación y capacitación en seguridad de la información**	¿Reciben los empleados y usuarios de terceras partes la formación apropiada, relativa a políticas y procedimientos de seguridad?		**x**									**x**	

Respuesta ante incidentes	**Comunicación de las incidencias de seguridad**	¿Existe un canal a través del que se reporten los incidentes de seguridad?		x				x					x
	Comunicación de las debilidades de seguridad	¿Se solicita a los usuarios que comuniquen cualquier debilidad de seguridad o amenaza para el sistema?		x									x
	Comunicación de los fallos del software	¿Existen procedimientos para informar los fallos de software?	x										
	Aprendiendo de las incidencias	¿Se analizan los tipos, volúmenes y costes de los incidentes y fallos?		x								x	
	Procedimiento disciplinario	¿Existe un proceso disciplinario para tratar las violaciones de las políticas y procedimientos de seguridad?		x						x			

Anexo 4. Cuestionario Seguridad Recursos Humanos

Seguridad física y ambiental														
Objetivo	**Control**	**Cuestión**	**Si**	**No**	**Parte**	**NS/NC**	**Presupuesto**	**Tecnología**	**Tiempo**	**No aplica**	**Entorno**	**Cultura**	**Desconocimiento**	**Otro**
Asegurar áreas	**Perímetro de seguridad física**	¿Existe un perímetro de seguridad para proteger las áreas donde están los sistemas?	x											
	Controles físicos de entradas	¿Están las áreas de seguridad protegidas por controles de entrada, para permitir el acceso sólo al personal autorizado?	x											
	Seguridad de oficinas, despachos y recursos	¿Están protegidos las oficinas y despachos que tienen algún requerimiento de seguridad especial?	x											
	El trabajo en las áreas de seguridad	¿Existen controles físicos especiales para trabajar en las áreas de seguridad?		x										x
	Áreas aisladas de carga y descarga	¿Están las áreas de entradas y salidas de mercancías aisladas del área de sistemas?		x								x	x	

Seguridad de los equipos	**Instalación y protección del equipamiento**	¿Están los equipos situados o protegidos para reducir las situaciones de riesgo o de acceso no autorizado?	**x**											
	Suministro eléctrico	¿Están protegidos los equipos contra fallos de corriente?	**x**											
	Seguridad en el cableado	¿Están protegidos contra daños o escuchas los cables que transmitan datos o soporten servicios de información?	**x**											
	Mantenimiento de equipos	¿Se mantienen los equipos en base a las recomendaciones del fabricante y/o procedimientos documentados?		**x**									**x**	
	Seguridad de equipos fuera de los locales de la organización	¿Existen procedimientos de seguridad y que cubran la seguridad de los sistemas cuando se usan fuera de las instalaciones de la empresa?		**x**									**x**	
	Seguridad en la reutilización o eliminación de equipos	¿Se borra la información de los equipos antes de reutilizarlos?	**x**											
Controles generales	**Política de puesto de trabajo despejado y bloqueo de pantalla**	¿Existe una política de pantallas y mesas limpias para los entornos de trabajo?	**x**											
	Sustracciones	¿Se necesita una autorización para sacar de las oficinas equipos, información o software?	**x**											

Anexo 5. Cuestionario Seguridad Física y Ambiental

Gestión de comunicaciones y operaciones															
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro

Procedimientos y responsabilidades de operación	**Documentación de procedimientos operativos**	¿Están documentados y mantenidos los procedimientos operacionales?		**X**					**X**						
	Control de cambios operacionales	¿Están controlados los cambios de los sistemas y aplicaciones?	**X**												
	Procedimientos de gestión de incidencias	¿Se han establecido procedimientos y responsabilidades, para la gestión de incidentes?		**X**										**X**	
	Segregación de tareas	¿Están segregadas las tareas, para reducir la oportunidad de o malos usos de los sistemas?	**X**												
	Separación de los recursos para desarrollo y producción	¿Están separadas las áreas de desarrollo y pruebas de las de los sistemas en operación?	**X**												
	Gestión de servicios externos	¿Se han identificado e incorporado al contrato los riesgos antes de utilizar servicios de terceros?		**X**											X
Planificación y aceptación del sistema	**Planificación de capacidades**	¿Se controla la necesidad de aumentar la potencia eléctrica, y la capacidad de proceso y almacenamiento?	**X**												
	Aceptación de sistemas	¿Existen criterios de aceptación para nuevos sistemas, ampliaciones o nuevas versiones?	**X**												
Protección contra software dañino	**Medidas y controles contra software dañino**	¿Existen procedimientos implantados para proteger a la empresa contra software malicioso?	**X**												
Gestión interna de respaldos y recuperación	**Recuperación de información**	¿Se hacen regularmente copias de seguridad?	**X**												
	Diarios de operación	¿Se mantiene un registro de las actividades del personal responsable de sistemas?		**X**					**X**						
	Registro de fallos	¿Se reportan los fallos del sistema y se toman acciones correctivas?	**X**												
Gestión de redes	**Controles de redes**	¿Se ha implantado algún tipo de control para mantener la seguridad en la red?	**X**												

Uso y seguridad de los soportes de información	**Gestión de soportes removibles**	¿Hay procedimientos para gestionar soportes removibles con información como discos, CDs, informes impresos,...?		**X**					**X**				**X**	
	Eliminación de soportes	¿Tienen procedimientos para asegurar el archivo y la destrucción de los soportes informáticos?		**X**									**X**	
	Procedimiento de uso de la información	¿Existen procedimientos para manejar y almacenar la información, que la protejan de malos usos?		**X**									**X**	
	Seguridad de la documentación de sistemas	¿Está la información y los documentos de sistemas protegidos de accesos no autorizados?	**X**											
Intercambio de información y software	**Acuerdos para intercambio de información y software**	¿Se han establecido acuerdos con otras empresas para intercambiar información o aplicaciones?	**X**											
	Seguridad de soportes en tránsito	¿Se toma alguna medida especial con los soportes en tránsito con información sensible?		**X**									**X**	
	Seguridad en comercio electrónico	¿Está protegido el comercio electrónico contra actividades fraudulentas (EDI, Email, transacciones on line, etc.)?		**X**									**X**	
	Seguridad del correo electrónico	¿Existe una política para el uso del correo electrónico?		**X**									**X**	
	Seguridad de los sistemas ofimáticos	¿Se han establecido políticas y directrices para controlar los riesgos de seguridad asociados con los sistemas dentro de las oficinas?		**X**									**X**	
	8.7.6. Disponibilidad de los sistemas públicos	¿Existe un proceso de autorización, para validar la información pública de la empresa antes de publicarla?	**X**											
	8.7.7. Otras formas de intercambio de información	¿Hay procedimientos y controles implantados para proteger el intercambio de información mediante voz, fax y video conferencia?		**X**									**X**	

Anexo 6. Cuestionario Gestión de Comunicaciones y Operaciones.

Control de accesos

Objetivo	Control	Cuestión	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Requerimientos de negocio para control de accesos	**Política de control de accesos**	¿Están documentadas las reglas y los derechos de acceso de los usuarios y los grupos?		**x**					**x**				**x**	
Gestión de acceso de usuarios	**Registro de usuarios**	¿Quedan registrados los accesos de los usuarios a los servicios y sistemas?	**x**											
	Gestión de privilegios	¿Está controlada la gestión de privilegios?	**x**											
	Gestión de contraseñas de usuario	¿Existe un proceso para la gestión de passwords de acceso a la información?	**x**											
	Revisión de los derechos de acceso de los usuarios	¿Se revisan periódicamente los derechos de acceso de los usuarios?		**x**										**x**
Responsabilidades de los usuarios	**Uso de contraseñas**	¿Se indica a los usuarios que sigan buenas prácticas en la selección y uso de passwords?		**x**									**x**	
	Equipamiento informático de usuario desatendido	¿Se solicita a los usuarios adoptar medidas de protección con los equipos desatendidos?		**x**									**x**	

Control de acceso en red	**Política de uso de los servicios de red**	¿Está garantizado que los usuarios sólo pueden acceder a los servicios para los que tienen autorización?		**X**							**X**			
	Ruta forzosa	¿Está controlada la ruta desde el Terminal de usuario al servicio del sistema?	**X**											
	Autenticación de usuarios para conexiones externas	¿Están autenticadas las conexiones de los usuarios remotos?		**X**											**X**
	Autenticación de nodos de la red	¿Están autenticadas las conexiones a sistemas remotos?		**X**											**X**
	Protección a puertos de diagnóstico remoto	¿Están controlados los accesos a los puertos de diagnóstico de los equipos del sistema?	**X**											
	Segregación en las redes	¿Esta la red segmentada por grupos usuarios y servicios?	**X**											
	Control de conexión a las redes	¿Está controlada la capacidad de conexión de los usuarios en redes compartidas?	**X**											
	Control de encaminamiento en la red	¿Tienen controles que verifiquen las direcciones de origen y destino de las conexiones en las redes compartidas?		**X**									**X**	
	Seguridad de los servicios de red	¿Están documentados los atributos de seguridad de todos los servicios de red?		**X**					**X**					

Control de acceso al sistema operativo	**Identificación automática de terminales**	¿Se identifican automáticamente los terminales, para autenticar las conexiones a localizaciones específicas y a equipos portátiles?		**X**									**X**	
	Procedimientos de conexión de terminales	¿El acceso a los sistemas se realiza mediante un logon seguro?		**X**									**X**	
	Identificación y autenticación de usuarios	¿Tiene cada usuario un identificador único?	**X**											
	Sistema de gestión de contraseñas	¿Existe un proceso para la gestión de passwords de accesos al SO?	**X**											
	Uso de utilidades del sistema	¿Están restringidos y controlados los programas de utilidades del sistema?	**X**											
	Protección de los usuarios frente a coacciones	¿Existen alarmas bajo coacción para acceso al SO?		**X**									**X**	
	Desconexión automática de terminales	¿Existen procedimientos y mecanismos para asegurar que se desconecten los terminales inactivos en localizaciones de riesgo?		**X**									**X**	
	Limitación del tiempo de conexión	¿Existen restricciones en las horas a las que se pueden realizar conexiones a aplicaciones de alto riesgo, así como en su duración?	**X**											
Control de acceso a las aplicaciones	**Restricción de acceso a la información**	¿Está restringido el acceso a la información y funciones del sistema de aplicación?	**X**											
	Aislamiento de sistemas sensibles	¿Están en un entorno aislado y dedicado los sistemas con información sensible?	**X**											

Seguimiento de accesos y uso del sistema	**Registro de incidencias**	¿Se mantienen durante un periodo de tiempo determinado los registros del sistema?	**X**												
	Seguimiento del uso de los sistemas	¿Existen procedimientos para monitorizar el uso de servicios de proceso de información?		**X**				**X**							
	Sincronización de relojes	¿Están sincronizados todos los relojes de los ordenadores?		**X**								**X**	**X**		
Informática móvil y teletrabajo	**Informática móvil**	¿Existe una política y los controles para proteger contra el riesgo de trabajar con portátiles?		**X**									**X**		
	Teletrabajo	¿Existen políticas y procedimientos para autorizar y controlar las actividades de tele trabajo?		**X**											**X**

Anexo 7. Cuestionario Control de Acceso

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.															
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Requerimientos de seguridad de los sistemas	**Análisis y especificaciones de los requerimientos de seguridad**	¿Se especifican los controles de seguridad necesarios para nuevos sistemas o mejoras de los actuales?		**x**									**x**	
Seguridad en sistemas de aplicaciones	**Validación de los datos de entrada**	¿Se validan los datos introducidos a las aplicaciones?	**x**											
	Control del proceso interno	¿Existen chequeos de validación incorporados en el sistema para detectar corrupciones de los datos procesados?	**x**											
	Autenticación de mensajes	¿Se ha implantado algún sistema de autenticación de mensajes?		**x**										**x**
	Validación de los datos de salida	¿Se valida la salida de datos de la aplicación del sistema?	**x**											

Controles criptográficos	**Política de uso de los controles criptográficos**	¿Existe una política de uso de controles de cifrado para la protección de la información?		**x**									**x**	
	Cifrado	¿Se aplica el cifrado para proteger la confidencialidad de la información crítica o sensible?		**x**									**x**	
	Firmas digitales	¿Se aplica la firma digital para proteger la autenticidad e integridad de la información?		**x**									**x**	
	Servicios de no repudio	¿Se emplean servicios de no repudio para resolver disputas sobre si algo ha ocurrido o no?		**x**									**x**	
	Gestión de claves	¿Se utiliza algún sistema de gestión de claves para soportar el uso de técnicas criptográficas?		**x**									**x**	
Seguridad de los ficheros del sistema	**Control del software en explotación**	¿Se aplica algún control para la implantar software en el sistema en operación?	**x**											
	Protección de los datos de prueba del sistema	¿Están protegidos los datos de prueba?	**x**											
	Control de acceso a la librería de programas fuente	¿Está controlado el acceso a las librerías de los programas fuente?	**x**											

Seguridad en los procesos de desarrollo y soporte	**Procedimientos de control de cambios**	¿Existen procedimientos para el control de cambios?		x									x	
	Revisión técnica de los cambios en el sistema operativo	¿Se revisan y aprueban los sistemas de aplicación cuando se producen cambios?	x											
	Restricciones en los cambios a los paquetes de software	¿Se desaconsejan las modificaciones de los paquetes de software?		x									x	
	Canales encubiertos y código troyano	¿Se controla y chequea adquisición, uso y cambios de sw con referencia a posibles puertas traseras y códigos troyanos?		x									x	
	Desarrollo externalizado del software	¿Se aplican controles para asegurar que el desarrollo subcontratado de software cumple con las medidas de seguridad necesarias?		x										x

Anexo 8. Cuestionario Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Gestión de Continuidad Comercial															
Objetivo	**Control**	**Cuestión**	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro
Aspectos de la gestión de la continuidad de negocio	**Proceso de gestión de la continuidad de negocio**	¿Existe un proceso establecido en la organización, para desarrollar y mantener la continuidad del negocio?		**x**									**x**	
	Continuidad del negocio y análisis de impacto	¿Existe un plan estratégico, basado en la valoración de riesgos, donde se detallen las acciones para la continuidad del negocio?		**x**									**x**	
	Redacción e implantación de planes de continuidad	¿Están desarrollados los planes de continuidad para mantener o restaurar las operaciones del negocio en un tiempo razonable?		**x**									**x**	
	Marco de planificación para continuidad del negocio	¿Existe un plan general de trabajo para asegurar que todos los planes son consistentes?		**x**									**x**	
	Prueba, mantenimiento y reevaluación de los planes de continuidad	¿Se prueban regularmente los planes de continuidad de negocio para asegurar que son eficaces?		**x**									**x**	

Anexo 9. Cuestionario Gestión de Continuidad Comercial

Conformidad legal															
Objetivo	Control	Cuestión	Si	No	Parte	NS/NC	Presupuesto	Tecnología	Tiempo	No aplica	Entorno	Cultura	Desconocimiento	Otro

Cumplimiento de los requerimientos legales	**Identificación de la legislación aplicable**	¿Están definidos y documentados, para cada sistema de información, todos los requisitos contractuales, reguladores y estatutarios?		**x**								**x**		
	Derechos de propiedad intelectual	¿Hay procedimientos para asegurar el cumplimiento con las restricciones legales en el uso de material referente a los derechos de propiedad intelectual?		**x**								**x**		
	Salvaguarda de los registros de la organización	¿Están protegidos contra pérdida, destrucción y falsificación los registros importantes?	**x**											
	Protección de datos de carácter personal y de la intimidad de las personas	¿Existen controles eficaces, para proteger la información personal en base a la legislación vigente?		**x**								**x**		
	Evitar el mal uso de los dispositivos de tratamiento de información	¿Existe autorización de la dirección para usar el sistema para fines no relacionados con el negocio (usos personales)?		**x**								**x**		
	Reglamentación de los controles de cifrado	¿Existen controles para asegurar el cumplimiento con los acuerdos		**x**									**X**	

Revisiones de la política de seguridad y de la conformidad técnica	**Conformidad con la política de seguridad**	¿Asegura la dirección que se siguen correctamente los procedimientos de seguridad, dentro de su área de responsabilidad?		**x**									**x**		
	Comprobación de la conformidad técnica	¿Se chequean regularmente los sistemas de información para verificar el cumplimiento con los estándares de implantación de seguridad?		**x**									**x**		
Consideraciones sobre la auditoría de sistemas	**Controles de auditoría de sistemas**	¿Están planificadas las auditorias de sistemas para reducir el riesgo de interrupciones en el proceso de negocio?		**x**									**x**		
	Protección de las herramientas de auditoría de sistemas	¿Esta protegido el acceso a las herramientas de auditoría del sistema?		**x**				**x**							

Anexo 10. Cuestionario de Conformidad Legal