-ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

MATERIA DE GRADUACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
ANALISTA DE SISTEMAS

TEMA:
"PROYECTO DE SEGURIDAD INFORMÁTICA PARA EL CONTROL DE ACCESO A REDES EN CIMA CONSULTING"

AUTORES:

MARIELA ZAMBRANO RODRÍGUEZ
DARÍO PALACIOS FRANCO

DIRECTOR:
MBA. VÍCTOR MUÑOZ CHACHAPOLLA

AÑO
2011

AGRADECIMIENTO

Damos gracias a Dios por habernos permitido alcanzar esta meta profesional que nos propusimos.

A nuestros padres que con amor y sacrificio nos acompañaron en cada paso de nuestras vidas estudiantiles y nos supieron conducir por el camino de los grandes ideales.

A nuestros amigos más cercanos que nos dieron todo su apoyo de manera incondicional.

A los profesores y compañeros que han iluminado y compartido cada uno de los rincones de nuestras etapas de estudios.

Mariela Zambrano

Darío Palacios

DEDICATORIA

Dedico este trabajo, que simboliza la culminación de una jornada más de mi vida, primero a Dios que me ha guiado por el sendero del bien y está conmigo en este triunfo, y me acompañara siempre.

A mis padres, hermanos y a todos quienes quieran compartir y han compartido conmigo las experiencias de esta etapa profesional.

Darío Palacios

DEDICATORIA

Dedico este trabajo a Dios que me ha permitido culminar está carrera profesional, a mi madre, hermanos, sobrinos y a todos quienes día a día comparten conmigo mis momentos de alegría, pero de manera personal a mi padre y hermano a quienes perdí en mí etapa final de estudios, quienes a la vez fueron mi fuerza para continuar y lograr esta meta.

Mariela Zambrano

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Trabajo Final de Graduación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FIRMA DEL DIRECTOR DE PROYECTO Y MIEMBRO DEL TRIBUNAL DE GRADUACIÓN

Mba. Víctor Muñoz Chachapolla
DIRECTOR DE PROYECTO

DELEGADO

FIRMA DE LOS AUTORES DEL PROYECTO DE GRADUACIÓN

Mariela Zambrano Rodríguez

Darío Palacios Franco

INTRODUCCIÓN

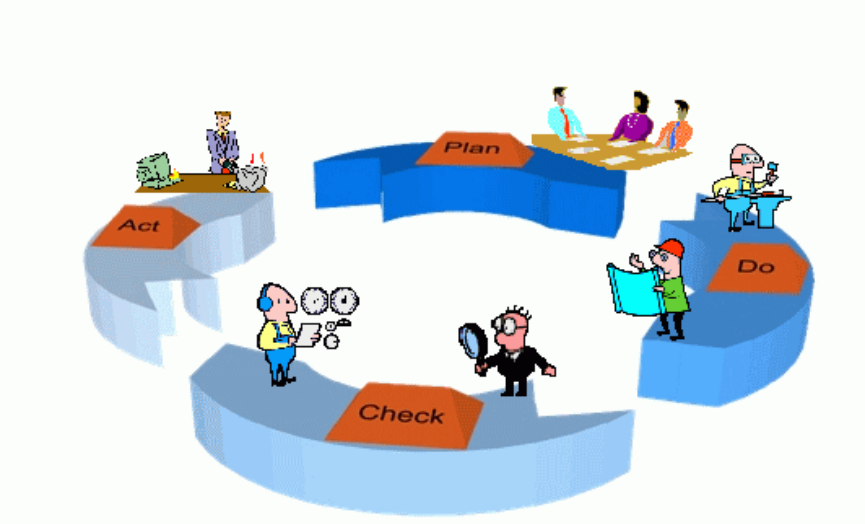
Este es nuestro documento de presentación, es donde se plantea la estructura recomendada que deberá tener el modelo de seguridad de la información (SGSI).

El presente trabajo trata el tema de la implementación de Control de Acceso a Redes. El trabajo comienza con una breve descripción de las distintas soluciones aplicables para realizar un excelente control de redes a la Empresa CimaConsulting basa en la norma ISO 27002.

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización que necesita ser tomado en cuenta. Una vez implementado este permitirá por medio de metodologías de análisis de riesgo, identificar las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de la red y, por otro lado, entender la importancia de definir políticas, procedimientos y estándares, de acuerdo a los requerimientos de la empresa.

Basados normativas recomendadas a nivel internacional según los estándares ISO 27002 hemos buscado identificar las herramientas o productos tecnológicos que apoyen los controles que permiten mitigar el riesgo y mejorar de esta manera la seguridad en la red.

Hasta el momento hemos identificado y definido las políticas que han sido y deberán ser implementadas para la correcta implementación de un sistema de seguridad de control de la red que brinde protección de la información que se maneja en la empresa.



Alcance SGSI

21/03/2011

Versión 1.1

Mariela Zambrano Rodríguez

Darío Palacios Franco

CONTROL DE CAMBIOS

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1.0	21/03/2011	SGSI001	SGSI Para redes	Modelo de Seguridad de la Información. Alcance, Políticas.
1.1	04/04/2011	SGSI002	SGSI Para redes	Modelo de Seguridad de la Información. Alcance, Políticas, Activos, Análisis de riesgos.
1.2	11/04/2011	SGSI002	SGSI Para redes	Modelo de Seguridad de la Información. Alcance, Políticas, Activos, Análisis de riesgos.
1.3	15/05/2011	SGSI002	SGSI Para redes	Correctivos del SOA.
1.4	20/05/2001	SGSI002	SGSI Para redes	Relación del DO y SOA por código distribuidos de manera ordena.

ÍNDICE GENERAL

ÍNDICE IMAGENES

ÍNDICE TABLAS

CAPÍTULO 1

DEFINICIÓN DE CONCEPTOS

1 DEFINICIÓN DE CONCEPTOS0

SGSI. La parte de un sistema global de gestión, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información (organización políticas. Incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Auditoria. Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Amenaza. Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Riesgo. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo Residual. El riesgo permanece tras el tratamiento del riesgo.

Política de seguridad. Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Plan de tratamiento de riesgos. Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Selección de controles. Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Vulnerabilidad. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Valoración de riesgos Proceso completo de análisis y evaluación de riesgos.

Tratamiento de riesgos. Proceso de selección e implementación de medidas para modificar el riesgo.

No conformidad. Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la medida para confidencialidad adecuación de las preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave. Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

ISO 27001. Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.

Inventario de activos. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)Dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de riesgos potenciales riesgos.

Integridad. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Incidente. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa descomprometer las operaciones del negocio y amenazar la seguridad de la información.

Impacto. El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros - pérdida de reputación, implicaciones legales, etc.

Gestión de riesgos. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Evento. Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evaluación de riesgos. Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Disponibilidad. Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Desastre. Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También se utiliza como sinónimo de salvaguarda o contramedida.

Control correctivo. Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control Preventivo Que evita ese riesgo. Produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Dirección IP. La dirección IP (Protocolo de Internet) de un ordenador es la serie de números con las que se identifica un equipo en la red, es algo parecido a: 192.168.0.99-cuatro grupos de cifras divididos por periodos. Una dirección IP es un título como si tuviera un número de teléfono asignado a un teléfono determinado.

Hub. Un hub de red es como el eje de la misma. Une las líneas de comunicación en un único lugar, ofreciendo una conexión común para todos los equipos y dispositivos de su

red. Con un hub, sus equipos están conectados entre sí pero no transmiten información pero no lo hacen con la misma rapidez que con un conmutador (switch).

Un conmutador o switch. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección de acceso de la máquina de destino de las tramas en la red.

Inalámbrico. Las redes inalámbricas pueden transmitir datos sin tener que tirar cables de un equipo a otro. Las redes inalámbricas tienen un alcance importante así que aunque se trate de espacios relativamente grandes puede obtener buenos resultados.

Latencia. La Latencia es el tiempo que tarda un equipo en iniciar una descarga (o cualquier otro tipo de información requerida). Es un poco diferente al ancho de banda. El ancho de banda es el tiempo que se necesita para mover/copiar la información. Si tiene una conexión con una latencia o tiempo de espera reducidos las descargas se inician antes. Sin embargo si tiene una conexión con un ancho de banda mayor el tiempo de descarga será inferior. Imaginemos por ejemplo una manguera de riego frente a una manguera de incendios: aunque la manguera de riego se pone en marcha con mayor rapidez, es decir tiene una "latencia" más baja que una manguera de incendios, esta última transmite más agua, dicho de otro modo, tiene un "ancho de banda" mayor.

Router. Un router es un dispositivo que se utiliza para conectarse a Internet en la mayoría de las redes. En algunos casos los routers tienen funciones de red incluidas. Gracias a los Routers se disfruta de comunicación en Internet, al tiempo que mantiene su actividad de red protegida del mundo exterior. Por lo general los Routers traen incluido un servidor de seguridad.

Router NAT con tecnología inalámbrica. Cuando tiene una red cableada (como Ethernet®) y además tiene una red inalámbrica, puede establecer un enlace entre ellas a través de un router NAT que tenga soporte para tecnología inalámbrica

Con este tipo de router, puede disfrutar de todos los beneficios de conectarse a la Red desde un equipo que está conectado de dos formas: con y sin cables. Por ejemplo puede que tenga una red conectada a Internet en casa y deba traerse trabajo a casa en el portátil

de vez en cuando. Un router NAT con soporte para conexión inalámbrica para conectar su portátil a la conexión de Internet que tiene en casa.

Software antivirus. El software antivirus le ayuda a saber qué hacer si algo o alguien ha conseguido entran a los servidores de seguridad. Por ejemplo, Los servidores de seguridad normalmente no captan los virus que se envían por correo electrónico. Dado que hay una amenaza constante de hackers creando virus y otros problemas de programas de software, siempre tiene que tener el software antivirus al día.

Tecnología de servidor de seguridad. Se han creado para ayudar a proteger los ordenadores personales al actuar como el guardián de la puerta y ayudar a asegurar que solo la información aprobada entra y sale del equipo. Y un servidor de seguridad verifica los permisos de cada paquete antes de permitir que siga su camino. Los datos entran y sales de los ordenadores a través de unas puertas a las que denominamos puertos. Debería utilizar un servidor de seguridad en cada pieza del equipo de la red, pero normalmente no debería ejecutar más de uno en un equipo determinado.

USB. El Puerto USB (Universal Serial Bus) es la alternativa a la interconexión de componentes periféricos (PCI). Todos los equipos de una red tienen que disponer de la tarjeta de red adecuada para poder comunicarse dentro de la red. Por lo general pueden obtener el tipo adecuado de tarjeta para su red en cualquiera de las clases de USB o PCI.

WPA. El Acceso Protegido Wi-Fi (WPA) es el estándar actual para la protección de información y seguridad en las redes inalámbricas. De este modo se evita que usuarios no autorizados se conecten a su red.

ACCESS POINT: (PUNTO DE ACCESO O AP). Es el dispositivo que hace de puente entre la red cableada y la red inalámbrica. Podemos pensar que es, de alguna manera, la antena a la que nos conectaremos. (También denominado un conmutador, un router o una estación base), todos los equipos de la red se comunican a través de ese dispositivo. Un punto de acceso actúa como una especie de estación central que gestiona toda la información que se envía a través de los equipos.

CUARTO DE EQUIPOS: Es un espacio centralizado dentro del edificio donde se albergan los equipos de red (ruteadores, switches, hubs, conmutadores, telefónicos, etc.), equipos de voz, video, etc.

SERVIDORES DNS: (DNS SERVER) Las páginas web también tienen su dirección IP pública y es a través de ésta dirección como en realidad nos conectamos a ellas. Pero claro, es más sencillo memorizar o escribir el nombre del dominio (www.google.es) que su dirección IP (216.239.59.104).

Para no memorizar la retahíla de números tenemos los servidores DNS. Un servidor DNS es un servidor en donde están almacenadas las correlaciones entre nombres de dominio y direcciones IP.

Archivo: Conjunto de información organizada localizada en el disco duro de una PC o un servidor.

BIOS: Basic Input-Output System, Sistema Básico de Entrada/Salida, es un código de software instalado en la placa base, en el cual se guarda la configuración de hardware y opciones de arranque de la computadora.

Correo electrónico: Mensajes electrónicos enviados o recibidos a través de Internet o de una red local de computadoras mediante un servidor de correo electrónico.

Equipo de cómputo: Término genérico que se utiliza en este manual, para denominar a una PC, impresora, scanner, disco duro, unidad de disquete, o cualquier otro componente de la computadora.

Freeware: Software de libre distribución y uso.

Ftp: (file transfer protocol) Protocolo de transferencia de archivos por medio de una red de computadoras con tecnología TCP.

Internet: Es una red mundial de computadoras interconectadas. Internet es la red de redes. Integra redes de área local (lan's, local área network) ubicadas en escuelas, bibliotecas, oficinas, hospitales, agencias federales, institutos de investigación y otras entidades, en una única red de comunicaciones extendida por todo el mundo.

Intranet; Es una red interna en un servidor web exclusivo y seguro, que le da al Personal de una institución o compañía, la posibilidad de compartir información.

Información, sin que ésta sea expuesta a la comunidad web en general.

Password o contraseña Es una cadena de caracteres que se usa para autentificar la identidad de un usuario. Cada contraseña está asignada a una cuenta o nombre de usuario para la autorización de acceso a la red.

Usuario Persona de cualquier área de la Secretaría del Medio Ambiente que requiere de un servicio o solución por parte del Área de Informática, para aprovechar las ventajas tecnológicas a favor de su trabajo.

1.1 MARCO DE REFERENCIA - SISTEMA DE GESTIÓN EN SEGURIDAD DE LA INFORMACIÓN SGSI

1.1.1 SEGURIDAD DE LA INFORMACIÓN

Se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

La seguridad de la información es la preservación de los principios básicos de la confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento. Estos tres pilares se definen como:

• **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados.

• **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• **Disponibilidad:** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. En la seguridad de la información, no solo intervienen los aspectos tecnológicos, sino también los procesos, los ambientes (centro de cómputo, ubicación de oficinas) y las personas.

1.1.2 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

La información contenida

Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

La infraestructura computacional

Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios

Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el

desempeño de los funcionarios y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

1.1.3 ¿QUÉ SIGNIFICA ENTORNO DE ARQUITECTURA DE SEGURIDAD?

• Gente, procesos y tecnología son las estructuras básicas de las organizaciones, siendo la más crítica la gente. La gente usa la tecnología para la construcción de procesos de negocio, por lo tanto estableciendo la interrelación entre las tres.

• Trabajamos con gente y a través de procesos y tecnologías para control, seguridad y mejora de sus entornos.

• La infraestructura es diseñada a través de tres fases del proceso - Estado Actual, Estado Deseado y Mejoras

• Cada una de las tres fases es usada para revisar los principales puntos de la seguridad en las políticas y procedimientos, tecnología y recupero y restauración.

• Luego la infraestructura nos lleva al segundo y tercer punto, aplicando las tres fases: Estado Actual, Estado Deseado y Mejoras.

• Con la primera fase del proceso, el análisis del estado actual y el grado a obtener es desarrollado.

• Mediante el cambio de parte de las personas, procesos o tecnología (y lo que es estático del entorno) el impacto caerá en seguridad en las áreas de Política y procedimientos, tecnologías y recupero y restauración.

• Los impactos en seguridad ante cambios en el entorno son difíciles sino imposibles de aislar.

• Con la segunda fase, se desarrolla un estado mejorado de infraestructura que es robusta y escalable.

• En la fase tres, el estado mejorado de seguridad es implementado e integrado para encontrar el entorno cambiado y las necesidades de la empresa.

En muchas empresas la función de tecnología informática ha evolucionado y crecido a través del tiempo, liderando o esperando cambios dentro de la organización. Mientras el desarrollo de una correcta arquitectura de seguridad debe corresponder a la situación actual de la organización, también necesita estar preparada para un estado innovador cuando sea apropiado.

1.2 ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION)

La ISO es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente encada país (entidad pública, privada).

La ISO desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros (previo consenso nacional entre industrias, expertos, gobierno, usuarios, consumidores) acerca de productos, tecnologías, sistemas y métodos de gestión, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación.

La ISO garantiza un marco de amplia aceptación mundial a través de sus 3.000 grupos técnicos y más de 50.000 expertos que colaboran en el desarrollo de estándares.

Estándar: publicación que recoge el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno y consumidores, que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

1.2.1 NORMA ISO27002

"Código de Buenas Prácticas para la Gestión de la Seguridad de la Información". Estructurada en 11 dominios desglosados en 133 controles, que cubren todos los aspectos fundamentales de la seguridad en el tratamiento de la información.

Figura 1- 1 *Control de acceso a redes ISO 27002*

1.2.2 DOCUMENTOS QUE PIDE LA NORMA ISO2002

- Alcance del SGSI
- Políticas objetivos de seguridad (se establecen los procedimientos de control)

- Procedimiento y mecanismo de control que soporta al sgsi
- Enfoque de la evaluación de riesgos
- Informe de los riegos
- Plan de tratamiento de riesgos
- Procedimiento de documentados
- Registros
- Declaración de aplicabilidad

1.2.3 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN –SGSI

Un SGSI es un Sistema de Gestión de la Seguridad de la Información o ISMS por sus siglas en inglés (Information Security Management System). Este sistema consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad.

1.2.4 BENEFICIOS DE LA IMPLANTACIÓN DE UN SGSI

Aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control, tratamiento y mejora en:

- **Aspecto Humano**: Mejora la sensibilización y responsabilidades del personal ante la seguridad en la organización.
- **Aspecto Financiero:** Reducción de los costos vinculados a los incidentes de seguridad.
- **Aspecto Organizacional:** Permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles.
- **Aspecto Funcional:** Gestión de los riesgos
- **Aspecto Legal:** Conformidad con leyes y normativas aplicables.
- **Aspecto Comercial:** Credibilidad y confianza de los socios, los accionistas y los clientes.

Ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de

contramedidas, por implantar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio.

- Definir Objetivos y Metas
- Integrar la Gestión de la Seguridad de la Información con el resto de sistemas de gestión existentes de la entidad.
- Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos, en su SGSI.
- Cumplimiento de la vigente sobre legislación protección de datos de carácter personal, comercio electrónico, etc.…
- Mejora continua de la gestión de la seguridad.
- Incremento de confianza de clientes.
- Garantía de continuidad del negocio.

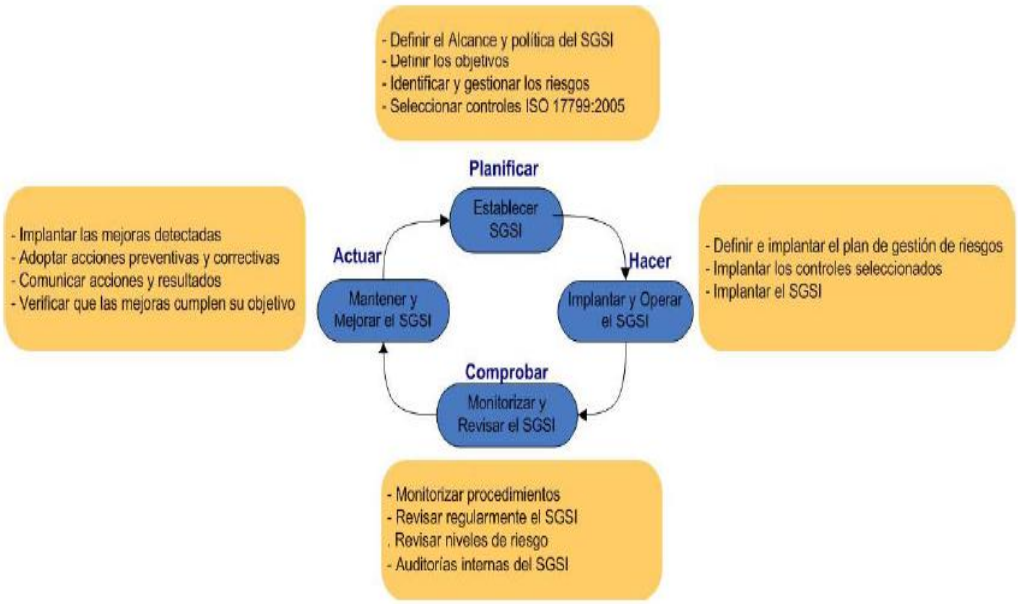


Figura 1- 2 Control de acceso a redes Ciclo

1.2.5 JUSTIFICACIÓN DE LA IMPLEMENTACIÓN DE UN SGSI

La información, junto a los procesos, y personas que hacen uso de ella, son activos importantes dentro de una organización. La confidencialidad, integridad y disponibilidad de información son elementos esenciales para mantener los niveles de

competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes –inherentes a los activos, pueden someter a los mismos a diversas formas de fraude, espionaje, sabotaje o vandalismo, entre otros. Los virus informáticos, el "hacking", pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas.

El nivel de seguridad alcanzado por medios y controles técnicos es limitado e insuficiente. En la gestión efectiva de la seguridad, debe ser apoyada por la Alta Dirección tomando en consideración también a clientes, proveedores de bienes y servicios. Este debe contemplar políticas y procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Modelo de gestión de seguridad de la información (SGSI) tiene como objeto mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un sistema SGSI, la organización conoce los riesgos a los que está sometida su información y activos y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Figura 1- 3 Justificación de la implementación de un SGSI

CAPÍTULO 2

EMPRESA

2 CIMA CONSULTING

Figura 2- 1 Logo Cima Consulting

Es una empresa desarrolladora de software que proporciona servicios profesionales de excelencia en consultoría de negocios basada en tecnología de información confiable eficiente y ética. Orientada a satisfacer las necesidades y aspiraciones de los clientes, en un esquema de total compromiso con los objetivos de sus clientes.

2.1 OPORTUNIDADES DE NEGOCIOS

La empresa Cima Consulting en los últimos meses ha tenido un mayor crecimiento en contratación de personal, adquisiciones de inmueble y equipos de cómputos, por lo que se visto en la necesidad de implementar seguridades en la red que no eran de tal importancia meses atrás, citando un ejemplo poseía 15 desarrolladores y actualmente cuenta con 70 aproximadamente,

Realizando un exhaustivo análisis pudimos notar que al no tener un control de seguridad de acceso a redes los recursos o desarrolladores están habilitados con salida a internet desobligándose de tareas laborales, esto está generando grandes pérdidas y descontentos de sus clientes al no poder cumplir con las fechas de compromiso en la entrega de un proyecto determinado.

2.2 ENUNCIADO DE LA VISIÓN DE CIMA CONSULTING

Ser una empresa de servicios en consultoría de negocios basada en tecnología de información. Claramente reconocida por su excelencia y su calidad. Así como por representar para quienes la integran. La mejor opción para desarrollar su vida profesional.

2.3 NECESIDADES DE DE CIMA CONSULTING

Cima Consulting no realiza un control de acceso a redes para evitar el uso indebido de las mismas lo que ha causando retrasos en los proyectos, congestión en la red, dificultades en el envío y recepción de los correos que son vitales para la constante comunicación que existen con los clientes.

No inspecciona que los usuarios solo tengan acceso a los servicios para los cuales han sido específicamente autorizados. Y los recursos o desarrolladores están habilitados con salida a internet desobligándose de tareas laborales, esto está generando grandes pérdidas y descontentos de sus clientes al no poder cumplir con las fechas de compromiso en la entrega de un proyecto determinado.

Además no protegen la información confidencial de la empresa lo que es un riesgo muy alto, Otro de los problemas es que en la empresa no posee un software o aplicación que permita el monitoreo de las acciones que realizan los empleados por la red, por lo que se debiera aplicarse registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes.

Por lo que se pueden requerir controles adicionales para proteger dicha información confidencial que pasa a través de redes públicas. La administración de redes además debe corregir estos inconvenientes; y mejorando la estructura empírica de la red (periféricos, hardware, etc.), logrando una mejor administración de redes que favorezca el caudal creativo y productivo de los usuarios.

2.4 DETALLE BREVE DE LOS SERVICIOS CIMA CONSULTING

- Ofrece Consultoría de sistemas orientados en sistemas CRM.
- Brinda el servicio de asesoría peopleSOFT
- Businessintelligent

2.5 ANÁLISIS DE BENEFICIOS

Metas	Objetivos	Beneficio
Implementar un sistema de Gestión para la seguridad de la red.	Implementar seguridades para el uso correcto de de la red siguiendo los estándares la norma ISO 27002.	• Los recursos o desarrolladores están habilitados con salida a internet con limitantes (políticas de seguridad). • Evitar grandes pérdidas y descontentos de sus clientes.

Tabla 2- 1 Metas, Objetivos y beneficio

CAPÍTULO 3

ETAPA DE PLANEACIÓN

3 ALCANCE

Los control de accesos según la norma ISO 27002 son: gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

Figura 3- 1 Control de acceso a redes ISO 27002

Control de Acceso de Red.- Prevenir el acceso no autorizado a los servicios de red.

A.11.4 Control De Acceso A Redes		
11.4.1	Política de uso de los servicios de red	Control: Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
11.4.2	Autentificación del usuario para conexiones externas.	Control: Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos
11.4.3	Identificación de equipos en las redes	Control: Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas

11.4.4	protección de puerto de Diagnóstico remoto	Control: Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración
11.4.5	Segregación en las redes	Control: Los servicios de información, usuarios y sistemas De información se deben segregar en las redes.
11.4.6	Control de conexiones de redes	Control: Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales
11.4.7	Control de encaminamiento de red	Control: Se deben implementar controles 'routing' para las redes redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones Comerciales.

Tabla 3- 1 Control de acceso a redes

3.1 MÉTRICAS:

- Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número
- De ataques potenciales de hacking repelidos, clasificados en insignificantes /preocupantes/críticos).

3.2 RESPONSABILIDADES:

La empresa está conformada por los siguientes responsables:

Jefe de sistemas.- es la persona responsable hacer cumplir las políticas, normas, pautas, y procedimientos de seguridad. También es responsable hacer las evaluaciones y adquisiciones e implantar productos de seguridad para la información, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, ingreso de hackers, hurtos y otros contratiempos.

El Jefe de red.- Responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la red, y de encontrar las soluciones a estos inconvenientes

El Administrador de Sistemas.- es quien establece los controles de acceso apropiados para cada usuario, supervisa el uso de los recursos, revisa bitácoras de acceso y de llevar a cabo las tareas de seguridad.

El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad.

Los usuarios.- son responsables de cumplir con todas las políticas de La compañía relativas a la seguridad informática. Tener conocimiento y aplicar los procedimientos sobre el manejo de la información. Cuidar su contraseña y evitar que sea vista por otros. No decir información confidencial de La compañía a personas no autorizadas o ajenas a la empresa

Notificar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier problema que afecte la seguridad de La compañía y sus recursos, como por ejemplo contagio de virus, intrusos, etc.

CAPÍTULO 4

DEFINICIÓN DE POLITICAS

4 POLÍTICA DE SEGURIDAD

Busca garantizar la confidencialidad de la información propia o proporcionada por nuestros clientes en relación a los servicios prestados. Garantizar la integridad, exactitud y veracidad de la información generada o procesada en la realización de los servicios.
Asegurar que el acceso a los sistemas de información relacionados con la prestación de los servicios, se realiza solamente por personal autorizado y con los privilegios de seguridad requeridos en relación al departamento o área a la que pertenece y según el desempeño de sus funciones.
Garantizar el cumplimiento de los acuerdos de nivel de servicio en relación a la seguridad de la información establecidos con terceros. Las políticas a aplicar son las siguientes:

- Uso aceptable de los activos
- uso contra software malicioso
- control de accesos
- uso de correo electrónico
- puestos de trabajo despejados
- uso de contraseñas de usuario
- uso de equipos portátiles

4.1 USO ACEPTABLE DE LOS ACTIVOS

- La información debe estar clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.
- Se considera información a todo dato relacionado con las actividades y servicios de una organización, que tenga valor para ésta según estime su propietario, atendiendo a las escalas de valoración utilizadas, los requisitos legales, su sensibilidad y criticidad para la organización, cualquiera sea su forma y medio de comunicación y/o conservación (información de los sistemas, documentos impresos,..)
- Toda información definida como activo debe ser clasificada para garantizar un nivel adecuado de protección. Los soportes (CD, papel, Discos Duros,…) que contengan información de distintos niveles de clasificación serán clasificados con el nivel más alto de los activos de información que contengan.

4.2 USO CONTRA SOFTWARE MALICIOSO

- No utilizar CD s, disquetes, memorias USB de fuera de las instalaciones en los equipos del sistema de información de la organización a menos que haya sido previamente verificado que están libres de virus u otros agentes dañinos.
- Los mensajes que se reciban de remitentes extraños o con contenido clasificable como no relacionable con la actividad empresarial deben ser eliminados en el acto, sin proceder a abrirlos.
- Estas acciones podrían suponer: Posibles infecciones por instalación de software no fiable. Violación de la Ley de Propiedad intelectual.
- Daño de información contenida en los equipos, como pérdida o modificación irreversibles.

4.3 CONTROL DE ACCESOS A LA INFORMACIÓN

- Verificar que se activa el protector de pantalla de manera automática y que la reanudación del trabajo implica la desactivación de la pantalla protectora con la introducción de la contraseña de usuario correspondiente.
- Guarde documentos y dispositivos de almacenamiento (CDs, memorias, etc.) con información crítica o sensible en armarios o los cajones bajo llave.
- No deje documentos a la vista, por ejemplo:
    - Nombre de Usuario y Passwords
    - Direcciones IP
    - Contratos
    - Números de Cuenta
    - Listas de Clientes
    - Propiedad Intelectual
    - Datos de Empleados/ Currículums.
- El identificador de usuario tendrá unos privilegios asociados, en función del cargo y las funciones que desempeñe. Los privilegios asociados a cada usuario le permitirán, en función de cada caso, acceder a un determinado tipo de información. El uso de un identificador único hace posible el seguimiento de las actividades realizadas por los usuarios, otorgando así responsabilidad individual sobre las acciones.

- No dejar funciones y equipos de soporte desatendidos, sobre todo si se va a imprimir o se está imprimiendo información confidencial de la empresa.

4.4 POLÍTICA DE USO DE CORREO ELECTRÓNICO

- Los usuarios que utilicen el correo electrónico dentro de la organización serán responsables de información. Evitar prácticas que puedan comprometer la seguridad de la información.

- Los servicios de email corporativos se suministran para servir a propósitos operacionales y administrativos relacionados con el negocio. Todos los emails procesados por los Sistemas de Información corporativos y redes son considerados propiedad de la organización.

4.5 NO USAR EL CORREO ELECTRÓNICO PARA:

- Enviar información confidencial/sensible, particularmente a través de internet, a menos que ésta sea primero cifrada por un sistema de cifrado aprobado por el Dpto. Informático.
- Para crear, enviar, reenviar o almacenar emails con mensajes o adjuntos que podrían ser ilegales o considerados ofensivos, sexualmente explícitos, racistas, difamatorios, abusivos, obscenos, discriminatorios u otros ofensivos.
- Para enviar un mensaje desde la cuenta de alguien o en su nombre (incluyendo el uso de una dirección falsa en el campo 'De').Si se autoriza por Dirección, una secretaria puede enviar emails en nombre de Dirección pero debería firmar el email en su propio nombre.
- Sea razonable sobre el número y tamaños de email enviados y guardados. Periódicamente elimine del buzón correos antiguos o que no vaya a necesitar más y clasifique los mensajes que necesite para mantenerlos bajo las carpetas apropiadas.

CAPÍTULO 5

EVALUACIÓN DE RIESGO

5 EVALUACIÓN DE RIESGO

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la Información sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Disponibilidad: Garantizar el correcto funcionamiento de los sistemas de información, así como de las tecnologías de comunicación.

Confidencialidad: Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.

Integridad: Garantizar que los datos sean los que se supone que son, es decir, que sean los correctos o no estén corruptos.

Y otros aspectos como:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.
- Se debe considerar la probabilidad de ocurrencia los posibles problemas. Con el fin de priorizar los problemas y así determinar cuáles son los problemas más constantes y necesiten mayor atención.
- Es de vital importancia tener conocimiento de lo que quiere proteger, para así reducir el impacto económico que pueda sufrir la empresa, o en su defecto que se vea afectado el servicio que brinda la misma.

Para el correcto uso de controles de seguridad, estos deben ser implementados en conjunto de manera arquitectónica. Con el fin de evitar afectar la integridad, disponibilidad y confidencialidad de los recursos de la empresa.

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, contabilidad, administración, etc.

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de

determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Figura 5- 1 Gestión de riesgos

Existen diferentes tipos de riesgos como el riesgo residual y riesgo total así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras.

El riesgo puede determinarse por medio de la siguiente fórmula:

$$\text{RIESGO} = \text{PROBABILIDAD} \times \text{IMPACTO}$$

Por medio de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el Riesgo Residual.

5.1 GESTIÓN DE RIESGOS

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo

En su forma general contiene cuatro fases.

Análisis: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro.

Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables para la empresa.

Reducción: Define e implementa las medidas de protección para mitigar el riesgo. Se podría capacitar a los usuarios para evitar que sucedan los mismos problemas.
Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las reglas, para determinar si es necesario ajustar las medidas ineficientes e inclusive se podría sancionar el incumplimiento en caso de no aplicar la norma o recomendación asignada.

5.1.1 PASOS PARA REALIZAR EL GESTIÓN DE RIEGOS

- Identificación de los activos que posee CimaConsulting.
- Valoración de los activos identificados
- Tener en consideración el impacto que se genere al momento de afectarse de manera negativa la confidencialidad, disponibilidad e integridad de los activos.
- Identificar cuáles son las amenazas y vulnerabilidades de los activos.
- Evaluación del riesgo según ocurrencia e impacto.

Después de efectuar el análisis de riesgo debemos determinar las acciones a tomar respecto a los riesgos que se identificaron y sus respectivas acciones para mitigarlos las mismas que por su ocurrencia podrían ser:

Controlar el riesgo.- Fortalecer los controles existentes y/o agregar nuevos controles de seguridad.

Desligar el riesgo.- Mediante acuerdos contractuales el riesgo se traspasa a un tercero.

Aceptar el riesgo.- Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

Eliminar el riesgo.- Eliminar el activo y con ello se elimina el riesgo.

5.1.2 RECOMENDACIONES

- Este necesario realizar un seguimiento continuo a los riesgos detectados, para que estos sean evaluados periódicamente.
- Capacitar al personal, creando políticas basadas en estándares, analizando grietas en la seguridad de un sistema de información.
- La recreación de escenarios de conflictos en forma continua participando los diferentes departamentos de la organización inclusive con la gerencia de la empresa, ayudara a mantener controlado el acceso a redes.
- Una vez terminado este proceso se debe documentar toda la información recopilada para su posterior análisis.

5.2 CLASIFICACIÓN DE LOS ACTIVOS

Hardware / Software

- Access Point
- Servidor
- Routers
- Switches
- Firewalls
- Proxy
- Correo electrónico.(Mail Security)
- Dispositivos anti-spyware
- 70 computadores
- 70 puntos de red

Personal

- 62 Desarrolladores

Figura 5- 2 Clasificación de activos

5.3 TABLA DE IDENTIFICACIÓN DE ACTIVOS

TABLA IDENTIFICACION DE ACTIVOS		
Categoría	**Nombre**	**Descripción**
HARDW (Hardware)	PC	Computador Personal
	NETWORK	Servidor de Proxy Server
	PRINT	Medios de Impresión
	SWITH	Conmutadores
	SERVIDOR	Alojamiento de información
	ROUTER	Enrutador
SOFTW (Software)	ANV	Antivirus
	CORREO	Cliente de correo electrónico
	BROWSER	Navegador Web
	FIREWALL	Pared corta fuegos
RED (Redes de comunicaciones)	PSTN	Red Telefónica
	PP	Red Inalámbrica
	LAN	Red Local
	INTERNET	Internet
	PTH	Patch Panel
ADD (Equipos adicionales)	CABLING	Cableado

Tabla 5- 1 Identificación de activos

5.4 TABLA DE INVENTARIOS DE ACTIVOS

CLASIFICACION DE LOS ACTIVOS			
Categoría	**Nombre**	**Descripción**	**Propietario**
HARDWARE	PT	• Procesador Intel Pentium Dual Core 3.0 Ghz Doble Nucleo • Mainboard Biostar g41 ddr3 chip intel • Memoria Ram 2Gb DDR3 • Disco Duro 500Gb Sata • Case Atx Negro • Teclado, Parlantes, Mouse • CDROM 22x • Monitor lcd 16''	DEPT.DESARROLLO
		• Intel® Pentium® Dual-Core E2220 • Memoria DDR 667 1 GB • Disco Duro 180Gb • CDROM 22x • Monitor lcd 16''	DEPT. RRHH
		• Intel® Pentium® Dual-Core E2220 • Memoria DDR 667 1 GB • Disco Duro 180Gb • CDROM 22x • Monitor lcd 16''	DEPT.CONTABILIDAD FACTURACION.
		• Server Ntel xeon quad core turbo 2.4ghz • 8 GB Memoria ram expandible a 16gb • Disco duro 500 sata 7200 rpm marca dell 3.5" (soporta hasta 4 discos internos) • Medios ópticos • Dvd /cd rom sata (una bahia lible adicional de 5.25") • Controladora sata 4 canales con opción de raid 1 y 0 • Teclado expandido dell usb	DEPT.SISTEMAS Y REDES

HARDWARE	PT	• Impresora HP LaserJet Pro CP1525nw a Color Usb 2.0 Red Lan Wi-FI	DEPT.DESARROLLO
		• Proxy Server (S.O. Linux, procesador PENTIUM 4, 512 MB)	DEPT. RRHH
		• Proxy Server (S.O. Linux, procesador PENTIUM 4, 512 MB)	DEPT.CONTABILIDAD FACTURACION.
		• MAIL Server (S.O. Linux + Lotus Domino, procesador PENTIUM 4, 512 MB).	DEPT.SISTEMAS Y REDES
SOFTWARE	CORREO	• Ooutlook .	TODOS LOS USUARIOS
	BROWSER	• Internet Explorer • Glooge Chrome	TODOS LOS USUARIOS
	AV	• Nod32	TODOS LOS USUARIOS
	FIREWALLE	• Sistema Operativo.	DEPT.SISTEMAS Y REDES
RED	PSTN	• Cableado estructurado categoría 5 - 6. UTP	DEPT.SISTEMAS Y REDES
	LAN	• Red LAN CON 48 puertos con una velocidad de 156 Gbps	DEPT.SISTEMAS Y REDES
	INTERNET	• IPv6 e Internet 2., con plataformas de fibra óptica cuyas capacidades exclusivas para esta red van en el orden de 1 Gbps	DEPT.SISTEMAS Y REDES
	PTH	• Patch Panel Universal GigaMax Categoría 5e de 48 puertos con etiquetado centralizado.	DEPT.SISTEMAS Y REDES
PER	PERSONAL	• Personal de redes	DEPT.SISTEMAS Y REDES
ADD	CABLING	• Puntos de RED	DEPT.SISTEMAS Y REDES

Tabla 5- 2 Inventario de activos

5.5 INVENTARIO DETALLADO DE ACTIVOS

Ubicación:	Dpto. Desarrollo	**Responsable:**	Jimmy Alvarado
		Cargo:	Ingeniero en desarrollo.
Descripción:			
• Elaboración de los diferentes manuales y documentación que exigen cada uno de los clientes ejemplo: * diagrama de procesos * Diagrama de estados * manual de Diseño * acta de entrega del proyecto • Desarrollo del proyecto o proceso asiganado • Pruebas del proyecto Instalación de la aplicación.			
Características			
• PC Escritorio.			

Tabla 5- 3 Inventario de activos Ing. en desarrollo

Observaciones: Cabe acotar que 20 máquinas con estas características, están destinadas al mismo uso y carga de trabajo con diferentes responsables.

Ubicación:	Dpto. Desarrollo	**Responsable:**	Darío Palacios
		Cargo:	Líder de Proyectos
Descripción:			
• Identificar los requerimientos de información de los clientes. (gerente) • Controlar y supervisar a los ingenieros en desarrolla que labora en el departamento • Tener a cargo la administración de los proyectos(gerente) • Contribuir a la mejora constantes de procesos. • Planificar ejecuciones y monitoreo de actividades del proyecto. • Elaborar actas de entrega del producto terminado			
Características General.			
• Laptop.			

Tabla 5- 4 Inventario de activos Líder de Proyectos

Observaciones: Cabe acotar que 12 máquinas con estas características, están destinadas al mismo uso y carga de trabajo con diferentes responsables.

Ubicación:	Dpto. Desarrollo	**Responsable:**	Manuel Pilco
		Cargo:	Gerentes de Proyectos
Descripción:			
• Identificar los requerimientos de información de los clientes. • Controlar y supervisar a los Lideres de proyectos que laboran en el departamento • Tener a cargo la administración y gerencia de los proyectos, • Elaborar actas de entrega del producto terminado • Planificar cronogramas para cada proyecto.			
Características General.			
• Laptop.			

Tabla 5- 5 Inventario de activos Gerentes de Proyectos

Observaciones: Cabe acotar que 4 máquinas con estas características, están destinadas al mismo uso y carga de trabajo con diferentes responsables.

Ubicación:	Dpto. Financiero	**Responsable:**	Antón Villalta
		Cargo:	Jefe Financiero
Descripción:			
• Realizar ingresos y gastos de la empresa. • Revisar cuentas del departamento de proyectos • Controlar el cobro o anticipos solicitados por los colaboradores • Controlar y hacer seguimiento de movimientos bancarios • Llevar el control de anticipos por proyectos.			
Características			
• PC escritorio			

Tabla 5- 6 Inventario de activos Jefe Financiero

Observaciones: Cabe acotar que 2 máquinas con estas características, están destinadas al mismo uso y carga de trabajo con diferentes responsables.

Ubicación:	Dpto. Financiero	**Responsable:**	Marcos Marin
		Cargo:	Jefe Marketing
Descripción:			
• Ejecución de campañas publicitarias de la empresa • Elaborar un plan de publicidad y de reconocimiento de la empresa. • Elaborar afiches publicitarios y publicaciones en medio escrito. • Elaborar carpetas de presentación de la empresa para sus clientes.			
Características			
• PC escritorio			

Tabla 5- 7 Inventario de activos Jefe Marketing

Observaciones: Cabe acotar que 2 máquinas con estas características, están destinadas al mismo uso y carga de trabajo con diferentes responsables.

Ubicación:	Dpto. RRHH	**Responsable:**	Lucy Suastegui
		Cargo:	Jefe Recursos Humano
Descripción:			
• Elaboración de rol de pagos: • Control y evaluación del desempeño • Elaboración de pruebas psicologías y de aptitud.			
Características			
• PC escritorio			

Tabla 5- 8 Inventario de activos Jefe Recursos Humano

Ubicación:	Dpto. Financiero	**Responsable:**	Nelson Rodríguez
		Cargo:	Gerente General
Descripción:			
• Elaboración de presupuestos • Administración del personal • Relaciones públicas • Seguridad y seguros • Planificación del negocio financiero y de desarrollo • Manejo de crisis – Solución de conflictos • Administración del riesgo empresarial			
Características			
• Laptop			

Tabla 5- 9 Inventario de activos Gerente General

5.6 VALORIZACIÓN DE LOS ACTIVOS

Basándonos en el inventario de los activos de la empresa que anteriormente describimos, realizamos las valorizaciones de los mismos según su confidencialidad, integridad, disponibilidad.

Disponibilidad	
Valor	**Criterio**
1	Baja
2	Media-Baja
3	Media
4	Media-Alta
5	Alta

Tabla 5- 10 Criterios de valorización de activos según su Disponibilidad

Confidencialidad	
Valor	**Criterio**
1	Publica
2	Uso Interno
3	Privada
4	Confidencial
5	Alta Confidencialidad

Tabla 5- 11 Criterios de valorización de activos según su Confidencialidad

Integridad	
Valor	**Criterio**
1	No necesaria
2	Opcional
3	Importante
4	Necesaria
5	Indispensable

Tabla 5- 12 Criterios de valorización de activos según su Integridad

Resultado de la valorización de activos según encuesta realizada al personal de redes de la empresa CIMA CONSULTING.

Activo	Confidencialidad	Disponibilidad	Integridad
Servidor	5 – Alta	5 - Alta	5 - Alta
Access Point	5 – Alta	4 – Media Alta	5 - Media
Impresora	4 – Media Alta	4 – Media alta	3 – Media
Routers	5 – Alta	5 - Alta	4 – Media Alta
Switches	3 – Media	5 - Alta	4 – Media Alta
Puntos de red	2 – Media Baja	5 - Alta	2 – Media Baja
PC desarrollo	4 – Media	5 - Alta	5 - Alto
PC RRHH	5 – Alta	3 – Media	4 - Media Alta
Firewalls	3 – Media Alta	5 – Media Alta	5–Alta
Correo electrónico	5 – Alta	5 - Alta	4 – Media Alta
Dispositivos anti-spyware	3 – Media Alta	5 – Media Alta	5–Alta
Proxy	4 – Media Alta	5 - Alta	4 – Media Baja
Modulo de roles de pagos	5 – Alta	5 - Alta	5 - Alta
Administrador de red	5 – Alta	5 - Alta	5 - Alta
Aplicación que controla entrada y salida.	5 – Alta	5 - Alta	5 - Alta
PC contabilidad y facturación	5 – Alta	4 - Alta	5 - Media Alta

Tabla 5- 13 Valorización de activos

5.7 TABLA DE VALORIZACIÓN DE ACTIVO

ACTIVO	VALOR
HARDWARE	
Servidor	5
Access Point / AP	4.66
Impresora	3
Routers	4.66
Switches	4.33
Puntos de red	3
PC desarrollo	4.66
PC RRHH	4
PC contabilidad y facturación	4.66
SOFTWARE	
Firewalls	4.33
Correo electrónico	4.66
anti-spyware	4.66
Proxy	4.66
Aplicación para controlar entrada y salida de los empleados	4.33
Módulo de roles de pagos	5
PERSONAL	
Administrador de red	5

Tabla 5- 14 valorización de activos

5.8 REPRESENTACIÓN GRÁFICA DE LA VALORIZACIÓN DEL ACTIVO

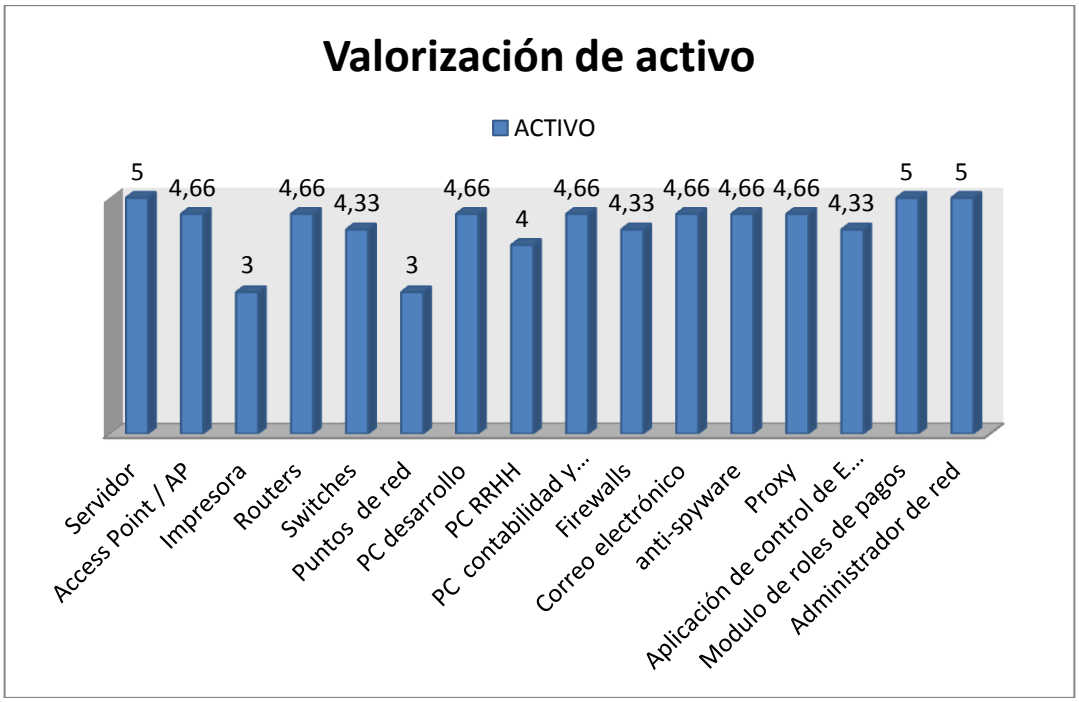


Figura 5- 3 Gráfico estadístico Valorización de riesgos

5.9 PLAN DE TRATAMIENTO DEL RIESGO:

Figura 5- 4 Gestión de riesgos

5.10 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación:

Sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

Desastres del entorno: dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones, incendios, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

5.11 LAS AMENAZAS

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer).

Un siniestro (robo, incendio, inundación): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

Figura 5- 5 Amenazas

5.12 AMENAZAS EN LA RED

Hoy en día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, y esta interconexión acarrea nuevas – y peligrosas – amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización (como un investigador que conecta desde su casa a través de un módem).

5.13 TIPOS DE AMENAZA

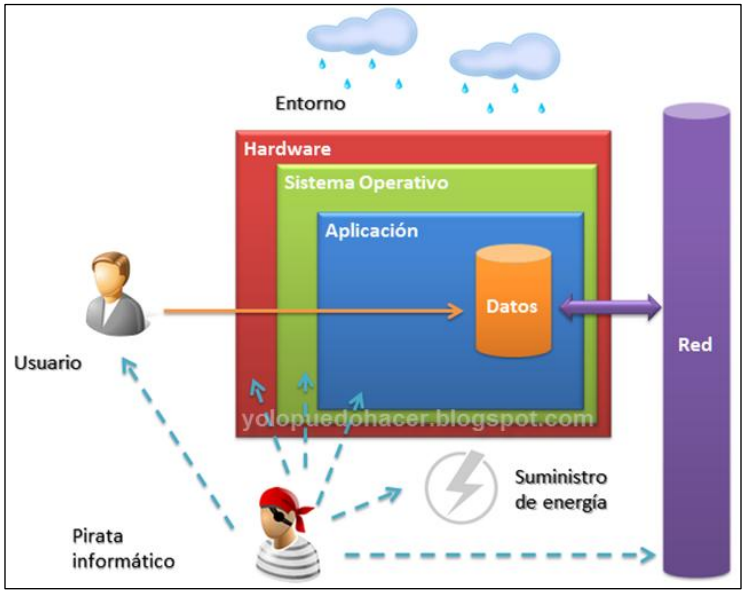


Figura 5- 6 Tipos de Amenazas

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. Basado en esto podemos decir que existen 2 tipos de amenazas:

5.13.1 AMENAZAS EXTERNAS

Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

5.13.2 AMENAZAS INTERNAS

Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

- Los usuarios conocen la red y saben cómo es su funcionamiento.
- Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

- Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares

5.14 LA AMENAZA INFORMÁTICA DEL FUTURO

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los significados de la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

Se puede afirmar que "la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas". Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información.

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o software espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

"La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas", La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital".

Para no ser presa de esta nueva ola de ataques más sutiles, Se recomienda:

1. Mantener las soluciones activadas y actualizadas.
2. Evitar realizar operaciones comerciales en computadoras de uso público.
3. Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.

5.15 PRINCIPALES AMENAZAS:

- Puertos vulnerables abiertos
- Mal asignación de permisos/ privilegios a usuarios
- Intercepción y modificación y violación de e-mails
- Descarga de Programas muy pesados.
- Acceso clandestino a redes
- Captura de PC desde el exterior
- Password cracking
- Virus
- Violación de contraseñas
- Empleados deshonestos
- Violación de la privacidad de los empleados ej. Sueldos, información personal, etc.
- Robo de información de personas internas o externas a empresa.

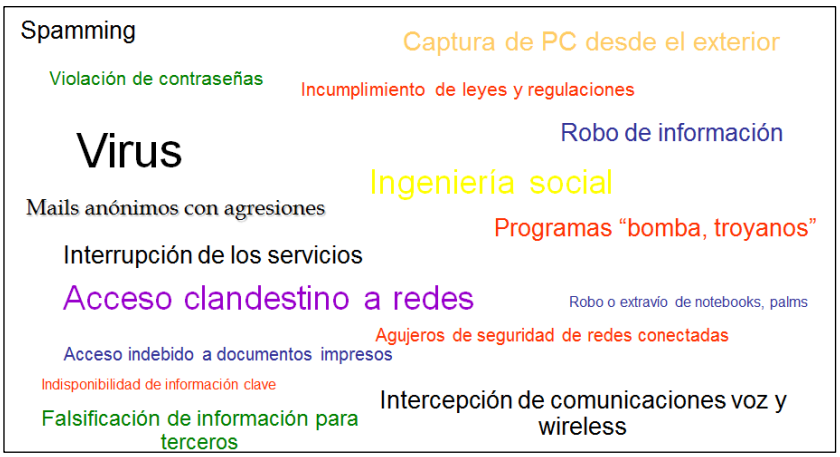


Figura 5- 7 Principales Amenazas

5.16 PRINCIPALES VULNERABILIDADES

- Personal inadecuadamente capacitado.
- Inadecuada asignación de responsabilidades.

- Ausencia de políticas/ procedimientos.
- Ausencia de controles (físicos/lógicos)
- (disuasivos/preventivos/detectivos/correctivos)
- Ausencia de reportes de incidentes y vulnerabilidades.
- Inadecuado seguimiento y monitoreo de los controles.
- Descargas de programas gran tamaño

5.17 CLASIFICACIÓN DE LOS RIESGOS

5.17.1 ACCESO FÍSICO

En este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos:

- Interrupción del suministro eléctrico.
- Apagado manual del equipo
- Vandalismo
- Apertura de la carcasa del equipo y robo del disco duro
- Monitoreo del tráfico de red

5.17.2 INTERCEPCIÓN DE COMUNICACIONES

- Secuestro de sesión.
- Falsificación de identidad.
- Re direccionamiento o alteración de mensajes.

5.17.3 DENEGACIONES DE SERVICIO

El objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:

Explotación de las debilidades del protocolo TCP/IP

Explotación de las vulnerabilidades del software del servidor

5.17.4 INTRUSIONES

- Análisis de puertos
- Elevación de privilegios: este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada

por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de desbordamiento de la memoria intermedia (búfer) usan este principio

- Ataques malintencionados (virus, gusanos, troyanos)

5.17.5 INGENIERÍA SOCIAL

En la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.

5.17.6 PUERTAS TRAMPA

Son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador en todo momento.

5.18 USO DEL ACTIVO

Frecuencia	Valor	Escala
A diario	Muy frecuente	5
Semanalmente	Frecuente	4
Mensualmente	Usualmente	3
Una vez al año	Poco frecuente	2
Cada varios años	Casi nunca	1

Tabla 5- 15 Niveles de frecuencia

5.19 TABLA DE EVALUACIÓN DE RIESGOS

EVALUACIÓN DE RIESGOS					
Activos	**Dpto.**	**Peligro identificado**	**Frecuencia**	**Impacto**	**Riesgo**

Servidor	Dpto. Redes	Corte de electricidad	2	5	10
		Acceso no Autorizado(Red)	2	5	10
		Acceso no Autorizado(Físico)	4	5	20
		Degradación de Hardware	2	5	10
		Ataque que atenta Hardware	2	5	10
Access Point	Dpto. Redes	Robo	1	4.66	4.66
		Escape de conexión	3	4.66	**13.98**
		Acceso no autorizado	1	4.66	4.66
		Análisis de trafico	3	4.66	**13.98**
Impresora	Dpto. Redes	Mal uso de la máquina	4	3	**12**
		Intenciones de acceder a imp.	4	3	**12**
		Hurto del dispositivos	5	3	**15**
Routers	Dpto. Redes	Degradación de Equipo	2	4.66	9.32
		Ataque que atenta Hardware	1	4.66	4.66
		Acceso a su configuración	4	4.66	**18.64**
		Análisis de trafico	3	4.66	**13.98**
Switches	Dpto. Redes	Degradación de Equipo	2	4.33	8.66
		Ataque que atenta Hardware	2	4.33	9.32
		Acceso a su configuración	1	4.33	4.33
		Análisis de trafico	2	4.33	8.66
		Degradación de Equipo	2	4.33	8.66
Pto. Red	Estableci_miento	Degradación del Punto	3	3	9
		Incidente que atenta cableado	4	3	12
PC	Desarrollo	Mal uso de la PC	2	4.66	9.32
		Intención de acceder a datos	5	4.66	**23.3**
		Hurto de dispositivos	4	4.66	18.64
		Sustracción de códigos fuentes	5	4.66	23.3
PC	Marketing	Mal uso de la PC	3	3	9
		Intención de acceder a datos	3	3	9
		Hurto de dispositivos	1	3	3
PC	Dpto. RRHH	Mal uso de la PC	2	4	8
		Intención de acceder a datos	1	4	4
		Hurto de dispositivos	1	4	4
		Acceso no autorizado	4	4	16

Tabla 5- 16 Evaluación de Riesgo

5.19.1 RESUMEN DE EVALUACIÓN DE RIESGOS

Resultados de Evaluación de Riesgos					
Activos	**Dpto.**	**Peligro identificado**	**Probabilidad**	**Impacto**	**Riesgo**
PC	Dpto.Cont. Fact.	Mal uso de la PC	2	4.66	9.32
		Intención de acceder a datos	4	4.66	18.64
		Hurto de dispositivos	1	4.66	4.66
		Acceso no autorizado	5	4.66	23.33
		Sustracción de Doc. Fact.	3	4.66	13.98
Correo Electrónico	Dpto. Redes	Mal uso del correo	3	4.66	13.98
		Robo.	2	4.66	9.32
		Escape de información	3	4.66	13.98
Aplicativo Control de Entrada	Puesto trabajo	Conexión Remota no controlada	5	4.33	21.65
		Acceso a su configuración	3	4.33	12.99
		Análisis de trafico	2	4.33	8.66

Tabla 5- 17 Evaluación de Riesgo

5.20 FÓRMULA PARA CALCULAR EL RIESGO

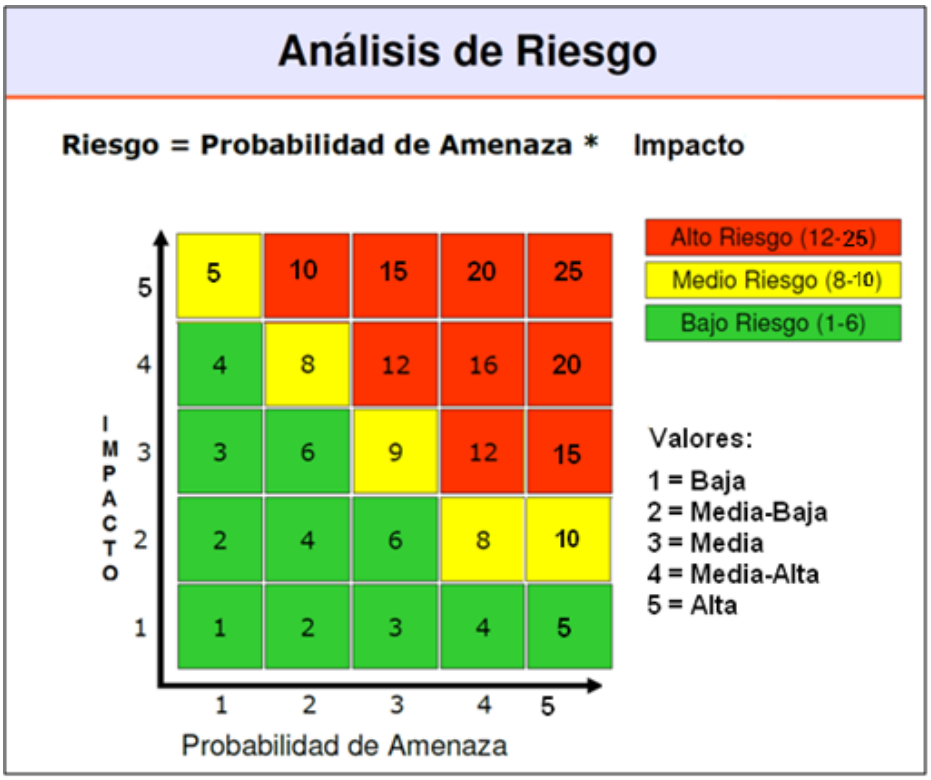


Figura 5- 8 Análisis de riesgo

CAPÍTULO 6

DO (Implementación)

6 DO –HACER

Es la fase de la implantación y operación de los controles procesos o procedimientos para el SGSI.

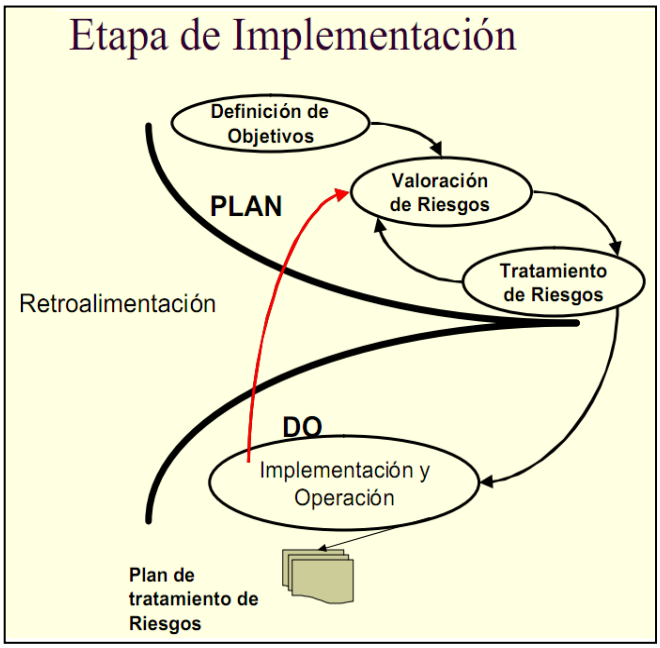


Figura 6- 1 Do (implementación)

1. Implementar y operar la política de seguridad, controles, procesos y procedimientos.
2. Implementar plan de tratamiento de riesgos.
3. Transferir, eliminar, aceptar
4. Implementar los controles seleccionados.
5. Mitigar
6. Aceptar riesgo residual.
7. Firma de la alta dirección para riesgos que superan el nivel definido.

6.1 CONTROLES

Son políticas, procedimientos, las prácticas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control correctivo. Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control Preventivo Que se evita el riesgo. Produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

6.2 PROCESOS

Un proceso es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado.

Código	Descripción	Objetivo
11.4.1	Política de uso de los servicios de red	Los usuarios sólo deberán disponer de acceso a los servicios que han sido específicamente autorizados a usar.
11.4.2	Autentificación de usuarios para conexiones externas	Métodos apropiados de autenticación se puede utilizar para controlar el acceso de usuarios remotos.
11.4.3	Identificación de equipos en las redes	Identificación del equipo automático se considerará como un medio para autenticar conexiones desde lugares específicos y equipos.
11.4.4	Protección de puerto y diagnóstico remoto	Acceso físico y lógico a los puertos de diagnóstico y configuración deben controlarse.
11.4.5	Segregación en las redes	Grupos de servicios de información, usuarios y sistemas de información deben estar separados de redes.
11.4.6	control de conexiones de red	Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, la capacidad de los usuarios conectarse a la red se limitarán, en línea con el acceso control de las políticas y requisitos de las aplicaciones de negocios.
11.4.7	Control de encaminamiento de red.	Se llevará a cabo por redes para asegurar que las conexiones de equipo y flujos de información no violen la política de control de acceso.

Tabla 5- 18 Controles de procesos

6.3 IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DEL RIESGO

El objetivo de este punto es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base al cuadro anterior y al capítulo anterior donde se encontraba la valoración de los riesgos:

Activo	Amenaza	Vulnerabilidades	PTR
PC de RRHH	Acceso de Personal No autorizado	Falta de políticas de control de acceso	Reducción
	Degradación o falla del punto de red	Falta de mantenimiento	Reducción
	Acceso a Internet	Uso de internet en oficina	Aceptable
PC de Marketing	Acceso de Personal No autorizado	Falta de políticas de control de acceso	Reducción
	Degradación o falla de HW	Falta de mantenimiento	Reducción
	Acceso a Internet	Uso de internet en oficina	Aceptable
	Uso de Internet	Falta de políticas de control de acceso a paginas no autorizadas Bloqueo de Páginas desde el departamento de Redes.	Reducción
PC de Desarrollo	Acceso de Personal No autorizado	Falta de políticas de control de acceso	Reducción
	Degradación o falla de HW	Falta de mantenimiento	Reducción
	Intención de acceder a datos	Falta de políticas de control de acceso	Reducción
	Infiltración de información	Falta de políticas de control de acceso	Reducción
	Sustracción de código fuentes	Falta de políticas de seguridad ya sea bloqueos de puertos	Reducción
	Acceso a Internet	Uso de internet para laborar	Aceptable
	Uso de Internet	Falta de políticas de control de acceso a paginas no autorizadas. Bloqueo de Páginas desde el departamento de Redes.	Reducción

Servidor	Negación del Servicio	Falta de personal capacitado para el control de servicios	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no adecuado del aire acondicionado	Reducción
	Degradación de HW	Falta de mantenimiento adecuado	Reducción
	Incumplimiento de controles de seguridad	Falta de conocimiento de seguridad por parte del software	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Ataque destructivo	Falta de protección física	Reducción
Red LAN	Acceso no autorizado a la información	Falta de control de acceso	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura	Reducción
Servicio de Correo electrónico	Análisis de tráfico	Falta de establecimiento de una conexión segura	Reducción
	Uso no previsto	Falta de Políticas	Reducción
	Fallas de servicios de soporte telefonía servicios de internet	Falta de acuerdos bien definidos con terceras	Reducción
Acceso Remoto	Acceso remoto Externo	Falta de procedimientos y seguridades en el control de acceso	Reducción
Desarrolladores	Errores de Empleados y acciones equivocadas	Falta de conocimientos y entrenamiento oportuno	Reducción
	Acceso a Internet	Uso de internet para laborar	Aceptable
	Uso de Internet	Falta de políticas de control de acceso a paginas no autorizadas Bloqueo de Páginas desde el departamento de Redes.	Reducción

Tabla 5- 19 Implementación tratamiento de riesgo

6.4 DECLARACIÓN DE APLICABILIDAD: (SOA -STATEMENT OF APPLICABILITY)

Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Para tener una excelente implementación de los controles también podrían considerar su nivel de madurez:

NIVEL DE MADUREZ DE UN CONTROL:

- Planificado (no ha sido implementado nada)
- Iniciado (Está en proceso)
- Implantado sin documentar (Ya está hecho pero falta documentarlo)
- Implantado para auditar (está implantado, documentado y estamos esperando que nos lo auditen para comprobar si cumple su objetivo o no).
- Auditado. (Proceso Finalizado)
- Se podrían agregar también: Revisado y mejoras:

Que nos indicarían si un control ha sido revisado y mejorado y y cómo se ha llevado a cabo dicha mejora en caso de que se haya producido.

Figura 6- 2 Aplicabilidad SOA

6.5 LOS CONTROLES A USAR SON LOS SIGUIENTES:

11.4.1 POLÍTICA DE USO DE LOS SERVICIOS DE RED

Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados Se debería formular la política de uso de las redes y los servicios de la red, que es conveniente que cubra: las redes y los servicios de la red a los que se puede acceder; los procedimientos de autorización para determinar quién puede acceder a qué redes y a qué servicios de la red; los controles y procedimientos de gestión para proteger el acceso a las conexiones de las redes y a los servicios de la red.

11.4.1.1 Se prohíbe la instalación de Software, Programas y/o Aplicaciones que comprometan el uso eficiente de la red y los equipos de cómputo.

11.4.1.2 El usuario no está autorizado para instalar o retirar cables o dispositivos de red.

11.4.1.3 En caso de ser requerido cualquier tipo de dispositivo de comunicaciones (Multipuertos, Ruterador, etc) el personal de Redes hará la instalación correspondiente con previa autorización del Director General o Ejecutivo.

11.4.1.4 Será responsabilidad total del usuario el uso de la información en su Equipo u otros recursos al compartirlos en la red.

11.4.1.5 Todo recurso compartido deberá tener contraseña o determinar que usuarios tendrán acceso, así como el tipo de permisos asignados,

11.4.1.6 Es responsabilidad del administrador de la red, el buen uso del software instalado en los equipos.

11.4.1.7 El personal que solicite o tenga a resguardo una computadora de escritorio, estación de trabajo, portátil, servidor, impresora, y/o cualquier otro dispositivo de entrada o salida, etc., se compromete a ser responsable por maltrato o mal manejo del mismo o alguno de sus componentes.

11.4.1.8 Se prohíbe almacenar cualquier tipo de información ajena al trabajo de la empresa (por ejemplo: archivos de música, imágenes, videos, etc.). En caso de que el personal autorizado localice este tipo de archivos tendrá la facultad de eliminarlos sin la necesidad de consultar al usuario.

11.4.1.9 La impresión por red, Las impresoras son de uso común y no personal por lo que se lo deberá hacer a la impresora del área que le corresponda. El

mantenimiento Correctivo y/o Preventivo de Hardware y Software y red será única y exclusivamente para el equipo propiedad de la empresa y realizado por el personal de Soporte Técnico.

11.4.1.10 En caso de requerir un mayor número de máquinas instaladas en un lugar donde sólo existe un nodo de red: Solamente el personal de Redes está autorizado a instalar hubs, switches y access point, previo estudio de factibilidad. En el caso de access point, con tarjetas de red inalámbricas que cumplan con los estándares internacionales de seguridad.

11.4.1.11 Está prohibido el acceso a los "Racks" ya que son áreas de equipamiento de redes, en los cuales se encuentra el cableado y el equipo de comunicación.

11.4.1.12 Los daños ocasionados al cableado y/o Rj de la red por negligencia del usuario serán directamente responsabilidad del mismo, comprometiéndose a cubrir el costo por la reparación de dichos daños.

11.4.1.13 En el caso de los servidores: El uso del servidor es estrictamente para labores propias de la empresa Cima consulting por lo cual los usuarios que tengan acceso a ellos no deberán utilizar sus recursos para fines personales (tales como almacenamiento de archivos, ejecución de programas, etc.).

11.4.1.14 Solamente el Director General, Ejecutivo o de Área, por medio de un oficio podrá hacer la petición del uso de los servicios para el personal que labore en su departamento, debiendo indicar los siguientes puntos:

Servidor que será accesado, Nombre del personal autorizado y recursos a accesar y justificación del mismo.

Privilegios a asignar.

El horario predeterminado de acceso a los servidores es de lunes a viernes de 8:00 a 21:00 hrs. En caso de necesitar un acceso diferente, deberá de ser especificado.

Tiempo que deberá permanecer activa la cuenta (por cuestiones de seguridad el máximo tiempo permitido será de 1 año, después de los cuales el usuario deberá renovar la petición de acceso).

11.4.1.15 El servidor llevan un registro detallado de las operaciones ejecutadas en el, por lo cual el usuario será responsable totalmente del buen o mal uso de

dichos recursos, así como pérdidas o cambios de información como resultados de errores de operación.

11.4.1.16 Al servidor se le realiza un respaldo en cinta todos los días sábado, el cual es resguardado por un periodo de dos semanas de operación, siendo responsabilidad del personal de Redes dicho respaldo. En caso de requerir que el respaldo se realice con una frecuencia diferente o se requiera un periodo mayor de almacenamiento, deberá solicitarse por escrito al personal de Redes correspondiente.

11.4.1.17 El personal de Redes es responsable de la integridad de los datos que los usuarios depositen en los servidores, sin embargo no será responsable por penalizaciones civiles o legales derivadas de la información resguardada.

11.4.1.18 En caso de requerir el respaldo de información específica que no esté contemplada dentro de los servidores, el usuario tendrá la obligación de notificarlo al personal de Redes a través de un oficio signado por su Director General, Ejecutivo o de Área, indicando la periodicidad de dicho respaldo, a fin de que se incluya en el compendio de información a resguardar en cinta.

11.4.2 IDENTIFICACIÓN DE EQUIPOS EN LAS REDES:

Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos. La autentificación de un usuario remoto puede realizarse utilizando, por ejemplo, una técnica basada en criptografía, símbolos de hardware o un protocolo de desafío/respuesta.

Un nodo de autentificación puede servir como un medio alternativo para autentificar grupos de usuarios remotos donde estén conectados a un computador seguro. Las conexiones externas proveen un potencial acceso no autorizado a la información del negocio, como los accesos mediante métodos de discado. Es necesaria la apropiada selección de un método de autentificación.

11.4.2.1 Asignar una dirección IP Número de identificación único a cada equipo conectado a una red de computo, de acuerdo con los estándares internacionales de la tecnología TCP, el cual es determinado por el administrador de la red en uso, por ejemplo, 191.31.140.115.

11.4.2.2 Sólo el personal de Redes, está autorizado para cambiar la configuración física y lógica de la red, es decir cables, Rj, direcciones IP, configuración de las impresoras compartidas en red, tipo de red, etc. Así como para asistir a los usuarios en problemas de comunicación.

11.4.2.3 Cima Consulting representada por el personal de red, tendrá la facultad de administrar, controlar, auditar, desarmar, reubicar el equipo según lo considere conveniente, para su mejor uso y aprovechamiento con la debida justificación.

11.4.3 PROTECCIÓN DE PUERTO Y DIAGNÓSTICO REMOTO

11.4.3.1 Se debería controlar el acceso físico y logístico para diagnosticar y configurar puertos. Controles potenciales para el acceso de diagnóstico y configuración de puertos incluyen el uso de un cierre con llave y de procedimientos de apoyo para controlar el acceso físico al puerto. Un ejemplo para dicho procedimientos de apoyo es asegurar que el diagnostico y configuración de puertos sean solo accesibles por arreglo entre el director del servicio de computo y el personal de mantenimiento de hardware/software que requiere acceso.

11.4.3.2 Muchos sistemas de computo, sistemas de red y de comunicación son instaladas con un diagnostico remoto o instalación de configuración para uso de ingenieros de mantenimiento.

11.4.4 SEGREGACIÓN EN LAS REDES:

Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes.

11.4.4.1 Un método para controlar la seguridad de grandes redes es dividirlas en dominios lógicos separados (por ejemplo dominios de redes internas a la organización o de redes externas), cada uno protegido por un perímetro definido de seguridad. Se puede aplicar un conjunto graduado de controles en diferentes dominios de redes lógicas para segregar a futuro los ambientes de seguridad de red, como por ejemplo sistemas públicos accesibles, redes internas y activos críticos. Los dominios deben ser

definidos basados en una evaluación de riesgos y los diferentes requisitos de seguridad entre cada uno de los dominios.

11.4.4.2 Los criterios para segregar las redes en dominios se deberían basar en la política de control de accesos y en los requisitos de acceso teniendo también en cuenta el costo relativo y el impacto en el rendimiento por la incorporación de la tecnología adecuada de enrutamiento de Gateway en la red.

11.4.4.3 Se debe tomar consideración con las redes inalámbricas desde una red interna hacia una privada. Como los perímetros de las redes inalámbricas no están bien definidos, se debe realizar una evaluación de riesgos en dichos casos para identificar controles para mantener una segregación de red. Las redes han sido crecientemente extendidas mas allá de las barreras organizacionales tradicionales, como se forman alianzas de negocios que puedan requerir la interconexión o el compartir las instalaciones de red y de procesamiento de información.

11.4.5 CONTROL DE CONEXIONES DE RED: USUARIOS, CONTRASEÑAS, DATOS Y ACCESO A LA RED

11.4.5.1 Las claves de acceso a la red constan de dos partes: una es la cuenta de usuario y la otra es la contraseña, por lo que las cuentas serán personales.

11.4.5.2 Todo usuario registrado en la red será responsable de proteger su nombre de usuario, contraseña y datos de cualquier acceso no autorizado.

11.4.5.3 Las cuentas de usuario registradas en la red son de carácter estándar, únicamente el personal de Redes, tiene los privilegios de modificar la configuración e instalación de aplicaciones adicionales a los equipos de cómputo.

11.4.5.4 Las claves de acceso serán habilitadas únicamente por el personal de Redes.

11.4.5.5 El usuario es responsable de su clave de acceso. Ninguna contraseña debe ser divulgada, escrita, enviada por correo electrónico y compartida por cualquier otra persona ajena al usuario, ya que esto se considera una violación a la seguridad de la red y si es detectado, se suspenderá la cuenta de red y se enviará un oficio informativo al titular del área a la cual está adscrito el usuario.

11.4.5.6 El usuario es responsable por las acciones que se lleven a cabo con su cuenta personal, es decir, las modificaciones a las bases de datos, archivos recibidos o enviados por correo electrónico, uso indebido de los recursos de la red.

11.4.5.7 Queda estrictamente prohibido el uso de un nombre de usuario distinto al propio, aun con el consentimiento del usuario original.

11.4.5.8 El personal de Redes definirá el número de usuarios con claves de acceso, este número podrá variar de acuerdo a solicitudes hechas por cada Dirección y las capacidades técnicas de la red. El número máximo de usuarios dependerá de la capacidad y direcciones IP disponibles en la red.

11.4.6 CONTROL DE ENCAMINAMIENTO DE RED:

El nivel de red se ocupa de que los paquetes que salen del transmisor lleguen a su destino, aunque el emisor y el receptor no estén adyacentes" (conectados directamente al mismo medio de transmisión).

Objetivo Encaminamiento De Red.

- Minimizar el espacio de la tabla de encaminamiento para poder buscar rápidamente y para tener menos información a intercambiar con otros encaminadores:
- Minimizar el número y frecuencia de mensajes de control Robustos.
- Evitar agujeros negros, evitar bucles, evitar oscilaciones en las rutas Generar caminos óptimos
- Menor retardo de transito, o camino más corto (en función de una cierta métrica en función de retardo, coste de los enlaces), o máxima utilización de la capacidad de la red

  Esto normalmente requiere pasar a través de nodos intermedios: encaminadores (routers). Por lo que se considera controlar lo siguiente:

11.4.6.1 Asignación de direcciones únicas a todas las máquinas de la red, independientes de la tecnología de los niveles de enlace.

11.4.6.2 Interconexión en una misma red de subredes con distinto nivel de enlace.

11.4.6.3 Control de congestión.

11.4.6.4 Servicio basado en Datagramas. La dirección de destino viaja en todos los paquetes de datos. El encaminamiento de cada paquete es independiente,

por lo que varios paquetes enviados del mismo origen al mismo destino pueden viajar por diferentes rutas (y, tal vez, llegar en desorden).

11.4.6.5 Servicio basado en Circuitos Virtuales Al principio se establece un \circuito virtual" por el que viajaran todos los paquetes de datos. La dirección de destino viaja sólo en los paquetes que establecen el circuito virtual. Los paquetes con datos solo llevan un identificador del circuito virtual al que pertenecen.

11.4.6.6 Todos los paquetes pertenecientes a un mismo circuito virtual siguen el mismo camino y llegan en orden.

11.4.7 APLICABLES A INTERNET

Todo el personal tendrá acceso al servicio de Internet. Cuando las necesidades del servicio así lo requieran, el Director General, Ejecutivo o de Área deberá solicitar por escrito al personal de Redes la habilitación del servicio de Internet para personal eventual, de honorarios. Esta solicitud deberá ser enviada a la Dirección.

A continuación se detallan algunos programas y acciones que no deben ser usados para el buen desempeño del servicio de Internet:

11.4.7.1 Chats, icq, bbs, irc, talk, write o cualquier programa utilizado para realizar pláticas en línea.

11.4.7.2 Cualquier programa destinado a realizar enlaces de voz y video, sin que esto sea previamente autorizado y justificado por la Dirección General, Ejecutiva o de Área.

11.4.7.3 Descargas de gran tamaño (mayores a 10 Mb) o uso de archivos de audio y multimedia.

11.4.7.4 Sitios de interacción social (redes sociales), páginas personales o aquellas que no tengan relación directamente con las labores propias del trabajo También se restringe el acceso a las páginas del tipo:

11.4.7.4.1 Dedicadas a proveer juegos en línea.

11.4.7.4.2 Con información que no sea relevante al trabajo del departamento.

11.4.7.4.3 Con material para adultos.

11.4.7.4.4 Dedicados a la difusión personal (Redes Sociales).

11.4.7.5 Servidores de almacenamiento masivo.