

UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA



**FACULTAD DE INGENIERÍA DE SISTEMAS
E INFORMÁTICA**



“Seguridad Informática”

INFORME DE TRABAJO PRÁCTICO DE SUFICIENCIA

**PARA OPTAR EL TITULO PROFESIONAL DE:
INGENIERO DE SISTEMAS E INFORMATICA**

**PRESENTADO POR EL BACHILLER:
NORMAN KARLSON FRIEDICH DIOPPE ARELLANO**

ASESOR:

ING. LUIS HONORATO PITA ASTENGO

IQUITOS – PERU

2015

**INFORME TECNICO DE EXAMEN DE SUFICIENCIA PREVIA
ACTUALIZACION ACADEMICA APROBADO EN SUSTENTACION PÚBLICA
EL DIA 13 DE ENERO DEL 2015, POR EL JURADO EXAMINADOR
DECIGNADO POR EL DECANO DE LA FACULTAD DE INGENIERIA DE
SISTEMAS E INFORMATICA DE LA UNIVERSIDAD NACIONAL DE LA
AMAZONIA PERUANA.**

.....
ING. CARLOS GARCIA CORTEGANO
PRESIDENTE

.....
ING. SAUL FLORES NUNTA
PRIMER MIEMBRO

.....
ING. CARLOS GONZALES ASPAJO
SEGUNDO MIEMBRO

.....
ING. LUIS H. PITA ASTENGO
ASESOR

RESUMEN

El presente trabajo tiene como objetivo, concientizar sobre la seguridad informática que se debe implementar tanto en las más grandes organizaciones o todo individuo en particular que maneja información de gran valor económico o personal, ya que en este mundo tecnológico que avanza a pasos agigantados debemos protegernos de los intrusos que merodean las redes de información, tratando de vulnerar la seguridades que están implementadas en los sistemas ya sea por el simple modo de curiosidad con la finalidad de perjudicar a alguna institución u individuo.

Para poder contrarrestar estos malos inconvenientes existen muchas soluciones en nuestra actualidad, con una gran cantidad de herramientas desarrolladas especialmente para cumplir con la función de proteger nuestra información, existe herramientas de con licencia propietario y otras que son software libre, cada una de ellas con sus diferentes características y valor económico.

Dependerá mucho de las políticas de seguridad de la empresa que se ha planteado, y del funcionamiento que estas realicen para poder adquirir un software que se adapte a sus respectivas necesidades, ninguna institución pública o privada está libre de ataques por más que se utilice las más grandes herramientas de protección ya que los Hackers cada día se inventan métodos de infiltración para vulnerar los sistemas de seguridad.

Por esta razón, y mediante el desarrollo de la presente trabajo se quiere apoyar con un pequeño estudio sobre una de las tantas herramientas, políticas, Estándares, procedimientos, que existen en nuestro medio, y al cual se ha rescatado la herramienta de seguridad informática “NESSUS”, “MAGERIT”, “COBIT”, el motivo de la selección de dicha herramienta es sencillo, pues nos ayuda a proteger nuestra red a grandes distancias y nos permite realizar auditorías remotas, y devolviéndonos resultados por si algún intruso está intentado vulnerar nuestra red.

INDICE

Resumen	iii
Índice.....	iv
I. Justificación.....	01
II. Objetivos	02
III. Desarrollo del tema	03
3.1 Seguridad Informática	03
3.1.1 Objetivo de la seguridad informática	03
3.1.2 Clasificación de la seguridad informática	03
3.1.2.1 Activa.....	03
3.1.2.2 Pasiva.....	03
3.1.3 Tipos de amenazas	03
3.1.3.1 Intercepción	04
3.1.3.2 Modificación.....	04
3.1.3.3 Interrupción.....	04
3.1.3.4 Generación	05
3.1.4 Herramientas de seguridad informática	05
3.1.4.1 Nessus.....	05
3.1.4.2 Magerit.....	06
3.1.4.3 Cobit	07
3.2 Seguridad física.....	07
3.2.1 Objetivo de la seguridad física.....	07
3.2.2 Prioridades de la seguridad física.....	08
3.2.3 Factores que afectan la seguridad física	09
3.2.3.1 Factores ambientales	10
3.2.3.2 Factores humanos	10
3.2.4 Entorno de hardware	11
3.2.4.1 Suministro de energía	11
3.2.4.2 Interconexión de redes y sistemas	12
3.2.4.3 Acceso físico al sistema	13
3.2.4.4 Ubicación del hardware	13
3.2.4.5 Control de acceso del personal al hardware	14
3.2.4.6 Sistema de control de hardware y su integridad.....	14
3.2.4.7 Desastres a nivel de hardware	15
3.2.4.8 Evacuación de hardware	15
3.2.4.9 Del personal con su interacción con el hardware	16
3.2.4.10 Monitorización del entorno	17
3.2.4.11 Cableado eléctrico.....	18
3.2.4.12 Cableado de telefonía	19
3.2.4.13 Cableado de redes	19
3.2.4.14 Sistemas distribuidos	20
3.2.4.15 Llaves, cerraduras y armarios	20
3.2.4.16 Cámaras de seguridad y monitorización	21
3.2.4.17 Control de ventanas y visibilidad desde el exterior.	21
3.2.4.18 Control de desechos y basura	22
3.2.5 Seguridad del hardware	23
3.2.5.1 Acceso físico a las máquinas y dispositivos de red..	23

3.2.5.2	Caja de la computadora	24
3.2.5.3	Seguridad de la BIOS.....	24
3.2.5.4	Equipamiento hardware de las maquinas.....	25
3.2.5.5	Acceso al interior de los equipos	26
3.2.5.6	Control de calidad de las máquinas y dispositivos de red	26
3.2.5.7	Control y seguridad de portátiles	27
3.2.5.8	Concentradores, bocas de red y conectividad.....	28
3.2.5.9	Grabación de datos, grabadores de cd, disqueteras	29
3.2.5.10	Dongles usb y sistemas de almacenamiento usb...	29
3.2.5.11	Sistemas de radio frecuencia. Tecnología Wireless y bluetooH.....	30
3.2.5.12	Dispositivo de mano. Palms y pocketPcs	31
3.2.5.13	Control de acceso del personal externos contratado al hardware.....	31
3.3	Seguridad Lógica	32
3.3.1	Objetivos de la seguridad lógica.....	32
3.3.2	Controles de acceso.....	33
3.3.2.1	Identificación y autenticación	33
3.3.2.2	Roles	33
3.3.2.3	Transacciones	33
3.3.2.4	Limitaciones a los servicios	34
3.3.2.5	Modalidad de acceso.....	34
3.3.2.6	Ubicación y horario	34
3.3.2.7	Control de acceso interno	35
3.3.2.7.1	Palabras claves.....	35
3.3.2.7.2	Encriptación	35
3.3.2.7.3	Listas de control de acceso	35
3.3.2.7.4	Limites sobre la interface de usuario	36
3.3.2.7.5	Etiqueta de seguridad	36
3.3.2.8	Control de acceso externo	36
3.3.2.8.1	Dispositivo de control de puerto.....	36
3.3.2.8.2	Firewalls o puertas de seguridad	37
3.4	Premisas Básicas de Seguridad	37
3.4.1	Integridad	37
3.4.2	Confidencialidad.....	37
3.4.3	Disponibilidad	38
3.4.4	No repudio.....	38
3.4.5	Autenticación.....	38
3.4.6	Autorización.....	39
3.4.7	Trazabilidad.....	39
3.4.8	Privacidad.....	39
3.5	Principios universales de la seguridad	39
3.5.1	Principio de menor privilegio	39
3.5.2	La seguridad no se obtiene a través de la oscuridad	40
3.5.3	Principio del eslabón más débil	40
3.5.4	Defensa en profundidad	41
3.5.5	Punto de control centralizado	41
3.5.6	Seguridad en caso de fallo	41
3.5.7	Participación universal	42

3.5.8 Simplicidad	42
3.6 Políticas y Mecanismos.....	42
3.6.1 Propósito de la política	42
3.6.2 Etapas en el desarrollo de una política	43
3.6.2.1 Fase de desarrollo	43
3.6.2.2 Fase de implementación.....	44
3.6.2.3 Fase de mantenimiento	46
3.6.2.4 Fase de eliminación.....	47
3.6.3 Mecanismos de la seguridad.....	48
3.6.4 Clasificación según su función	48
3.6.4.1 Preventivos	48
3.6.4.2 Detectivos	48
3.6.4.3 Correctivos	48
3.6.4.4 Huella digital	49
3.6.4.5 Verificación de voz.....	49
3.6.4.6 Verificación de patrones oculares.....	49
3.7 Documentación formal de la seguridad informática	50
3.7.1 Política	50
3.7.2 Estándar	50
3.7.2.1 Trusted Computer Security Evaluation Criteria. TCSEC	51
3.7.2.2 Information Tec Security Evaluation Criteria. ITSEC	54
3.7.2.3 ISO 15408 Criterios Comunes (CC)	55
3.7.2.4 BS 7799 (Reino Unido).....	56
3.7.2.5 ISO 17799	56
3.7.2.6 Los controles del ISO 17799	58
3.7.2.7 ISO 27000	60
3.7.3 Mejor practica.....	62
3.7.4 Guía	62
3.7.5 Procedimientos.....	62
IV. Conclusión	64
V. Referencias Bibliográficas.....	65
Anexos	66

I. JUSTIFICACION:

La Seguridad Informática es un problema complejo, no bien comprendido, mucho menos asimilado dentro de las prácticas actuales. Asegurar la información de una organización requiere la adecuada combinación de tecnologías, metodologías, estándares, herramientas gerenciales y en general del “Business-Sense”, de manera que no siempre es evidente el camino que debe tomar la alta gerencia con respecto al problema, cada vez más apremiante de garantizar la Seguridad de la Información.

La Seguridad Informática es relevante en áreas tecnológicas del entorno nacional e internacional, por lo tanto, en un consenso internacional, un experto en Seguridad de la Información en la industria, requiere no sólo conocer y saber aplicar adecuadamente elementos tecnológicos, tales como técnicas biométricas, técnicas criptográficas, modelos formales de seguridad, arquitectura del computador, sistemas operativos y redes, Políticas, Procedimiento; sino también herramientas gerenciales de planeación de continuidad, manejo de incidentes y recursos humanos, auditoría, seguridad física e incluso la adecuada comprensión de los aspectos legales de estos temas. Esto muestra la importancia de la seguridad informática dentro de las organizaciones o personalmente nos orientan hacia las líneas de la investigación como son Análisis Criptográfico, Sistemas Biométricos Avanzados, ISO27000, entre otras.

Las organizaciones muchas veces están expuestas a diferentes riesgos de la seguridad informática que existen en la actualidad, así que la importancia de minimizarlos para mantener la integridad, confiabilidad y disponibilidad de la información.

II. **OBJETIVOS:**

GENERAL:

Realizar una revisión general de los conceptos relacionados a la seguridad informática, mostrando su clasificación, políticas, mecanismos, procedimientos y la aplicación de estándares dentro de las organizaciones.

ESPECIFICOS:

- Dar a conocer las situaciones de riesgo, ataques y amenazas tanto físicas como lógicas que afectan la seguridad informática.
- Conocer los mecanismos de seguridad informática existentes.
- Determinar herramientas necesarias para el control de la seguridad informática.
- Utilizar de la manera correcta las políticas, mecanismos, estándares y procedimientos para tener una buena seguridad informática.
- Ampliar o enriquecer los conocimientos acerca de la seguridad informática.

III. DESARROLLO DEL TEMA

3.1 SEGURIDAD INFORMÁTICA:

Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. **(Morant, 1994).**

3.1.1 Objetivo de la seguridad informática

- Es proteger la infraestructura computacional.

3.1.2 Clasificación de la seguridad informática:

3.1.2.1 Activa

Se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema. **[Alfonso, 2011].**

- *Ejemplos:* podemos encontrar en el empleo de contraseñas, listas de control de acceso, encriptación, cuotas de disco duro, firmas y certificados digitales, uso de antivirus, cortafuegos o firewall, etc.

3.1.2.2 Pasiva

Complementa a la seguridad activa y se encarga de minimizar los daños en caso de que haya algún fallo o daño. **[Alfonso, 2011].**

- *Ejemplos:* conjuntos de discos redundantes, SAI's, copias de seguridad.

3.1.3 Tipos de amenazas

Las amenazas al sistema informático pueden también clasificarse desde varios puntos de vista.

En una primera clasificación según el efecto causado en el sistema, las amenazas pueden englobarse en cuatro grandes tipos: interceptación, modificación, interrupción y generación. Vamos a verlas con más detalle.

3.1.3.1 Interceptación

Cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Ejemplos:

- Escucha de una línea de datos.
- Copias de programas o ficheros de datos no autorizados.

Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información o el sistema.

3.1.3.2 Modificación

Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino, además, de cambiar en todo o en parte su contenido o modo de funcionamiento.

Ejemplos:

- Cambiar el contenido de una base de datos.
- Cambiar líneas de código en un programa.
- Cambiar datos en una transferencia bancaria.

3.1.3.3 Interrupción

Interrumpir mediante algún método el funcionamiento del sistema.

Ejemplos:

- aturar la memoria o el máximo de procesos en el sistema operativo.
- Destruir algún dispositivo hardware.

Puede ser intencionada o accidental.

3.1.3.4 Generación

Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema.

Ejemplos:

- Añadir campos y registros en una base de datos.
- Añadir código en un programa (virus).
- Introducir mensajes no autorizados en una línea de datos.

Como puede observarse, la vulnerabilidad de los sistemas informáticos es muy grande, debido a la variedad de los medios de ataque o amenazas. Fundamentalmente hay tres aspectos que se ven amenazados: el hardware (el sistema), el software (programas de usuarios, aplicaciones, bases de datos, sistemas operativos, etc.), los datos.

Desde el punto de vista del origen de las amenazas, estas pueden clasificarse en: naturales, involuntarias e intencionadas.

3.1.4 Herramientas de seguridad informática

3.1.4.1 Nessus

Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un daemon, *nessusd*, que realiza el escaneo en el sistema objetivo, y *nessus*, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola *nessus* puede ser programado para hacer escaneos programados con cron.

En operación normal, *nessus* comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos

abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en **NASL** (*Nessus Attack Scripting Language*, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos originalmente por gordon Lyon(más conocido por su alias *Fyodor Vaskovich*). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

3.1.4.2 Magerit

Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. Actualmente está en su versión 3.

Magerit ofrece una aplicación, **PILAR** para el análisis y gestión de riesgos de un Sistema de Información.

- R-Box: Herramienta de Análisis y Gestión de Riesgo basada en Magerit.
- GxSGSI: Herramienta de Análisis y Gestión de Riesgo basada en Magerit

Que tiene la finalidad de poder "dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información".

MAGERIT es por tanto un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad.

3.1.4.3 Cobit

El modelo de servicios, infraestructura y aplicaciones identifica las capacidades de servicios que se requieren para proveer seguridad de la información y funciones relacionadas a una empresa. La siguiente lista contiene ejemplos de servicios potenciales relacionados a seguridad que podrían aparecer en un catálogo de servicios de seguridad:

- Proveer una arquitectura de seguridad.
- Proveer una concientización de seguridad.
- Proveer evaluaciones de seguridad.
- Proveer una respuesta adecuada de incidentes.
- Proveer una protección adecuada contra malware, ataques externos e intentos de intrusiones.
- Proveer monitoreo y servicios de alerta para eventos de SI.

3.2 SEGURIDAD FÍSICA

La seguridad física es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso. **(José, 1997).**

3.2.1 Objetivo de la seguridad física

- Asegurar la capacidad de supervivencia de la organización ante eventos que pongan en peligro su existencia.
- Proteger y conservar los activos de la organización, de riesgos, de desastres naturales o actos mal intencionados.

- Reducir la probabilidad de las pérdidas, a un mínimo nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.
- Asegurar que existan controles adecuados para las condiciones ambientales que reduzcan el riesgo por fallas o mal funcionamiento el equipo, del software, de los datos y de los medios de almacenamiento.
- Controlar el acceso, de agentes de riesgo, a la organización para minimizar la vulnerabilidad potencial.

3.2.2 Prioridades de la seguridad física

¿Qué se quiere proteger?

Es muy importante determinar el valor del hardware y las tareas que realiza (qué tan importante es para la organización en que se está trabajando). Esta valoración debe hacerse de forma individual, pues lo que es valioso para algunos no lo es para otros.

¿Contra qué se quiere proteger?

Para no incurrir en gastos innecesarios, es importante determinar cuáles son los riesgos reales a los que está expuesto el equipo de cómputo. La seguridad efectiva debe garantizar la prevención y detección de accidentes, ataques, daños por causas naturales, así como la existencia de medidas definidas para afrontar los desastres y lograr el restablecimiento de las actividades.

¿Cuánto tiempo, dinero y esfuerzo se está dispuesto a invertir?

Se refiere a la cantidad de recursos que dispone o que está dispuesta a invertir la organización, lo que determinará en última instancia las medidas que se van a tomar.

Estos recursos son:

- **Tiempo:** Para tener un nivel de seguridad alto es necesario que alguien dedique tiempo a configurar los parámetros de seguridad del sistema, el ambiente de trabajo de los usuarios, revisar y fijar los permisos de acceso a los archivos, ejecutar programas de monitoreo de seguridad, revisar las bitácoras del sistema, etc.
- **Esfuerzo:** Establecer y mantener un nivel adecuado de seguridad puede significar un esfuerzo considerable por parte del encargado, sobre todo si ocurren problemas de seguridad.
- **Dinero:** El tener a alguien que se encargue de la seguridad en forma responsable cuesta dinero. De igual forma cuesta dinero adquirir los productos de seguridad que se vayan a utilizar, ya sean programas o equipos. Es importante también analizar los costos que tendrían la pérdida o acceso no autorizado a la información. Dependiendo de esto, y en el caso de que alguien tenga acceso no autorizado, el efecto pueden ser pérdidas monetarias.

3.2.3 Factores que afectan la seguridad física

Los riesgos ambientales a los que está expuesta la organización son tan diversos como diferentes sean las personas, las situaciones y los entornos. El tipo de medidas de seguridad que se pueden tomar contra factores ambientales dependerá de las modalidades de tecnología considerada y de dónde serán utilizadas. Las medidas de seguridad más apropiadas para la tecnología que ha sido diseñada para viajar o para

ser utilizada en el terreno serán muy diferentes a la de aquella que es estática y se utiliza en ambientes de oficina.

3.2.3.1 Factores ambientales

- **Incendios:** Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones inalámbricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.
- **Inundaciones:** Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.
- **Sismos:** Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan, o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.
- **Humedad:** Se debe proveer de un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y al área de máquinas en forma exclusiva.

3.2.3.2 Factores humanos

- **Robos:** Las computadoras son posesiones valiosas de las empresas, y están expuestas, de la misma forma que están expuestas las piezas de stock e incluso el dinero. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección de la que dan a una máquina de escribir o a una calculadora, y en general a un activo físico.

- **Actos vandálicos:** En las empresas existen empleados descontentos que pueden tomar represalias contra los equipos y las instalaciones. Actos vandálicos contra el sistema de red. Muchos de estos actos van relacionados con el sabotaje.
- **Fraude:** Cada año millones de dólares son sustraídos de empresas y, en muchas ocasiones las computadoras han sido utilizadas para dichos fines.
- **Sabotaje:** Es el peligro más temido en los centros de cómputo. Empresas que han intentado implementar sistemas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros, el saboteador puede ser un empleado o un sujeto ajeno a la empresa.
- **Terrorismo:** Hace unos años, este hubiera sido un caso remoto, pero con la situación bélica que enfrenta el mundo las empresas deben de incrementar sus medidas de seguridad, por que las empresas de mayor nombre en el mundo son un blanco muy llamativo para los terroristas.

3.2.4 Entorno hardware

Entendemos como entorno físico del hardware el entorno en el que está situado nuestro hardware, dispositivos de red y centros de computación. Es el paso siguiente en el estudio de la seguridad física al estudio de la edición. [Rusell, 1996].

3.2.4.1 Suministro de energía

Es imprescindible el asegurar un suministro estable y continuo de energía eléctrica al hardware, utilizando normalmente sistemas UPS (Sistema de suministro ininterrumpido de energía) que regularán la tensión evitando los picos de voltaje que pueda traer la red y

proporcionarán un tiempo de autonomía por medio de baterías en caso de cortes del suministro eléctrico.

Para evitar puntos de fallo es conveniente el no depender únicamente de un sistema UPS para todo el hardware a proteger, siendo más conveniente la instalación de varios UPS que puedan suministrar energía a parte del sistema en el caso de que uno de los UPS fallara. Se estudiará la autonomía de los UPS y las protecciones que proporcionan al hardware y se recomendará en su caso la instalación de más sistemas UPS o la redundancia de alguno de ellos.

3.2.4.2 Interconexión de redes y sistemas

Deberemos comenzar estudiando el diseño de la red del edificio, observando las troncales de red que intercomunicarán las diferentes plantas y secciones del edificio.

Una red típica de un edificio consta de uno o varios grandes enrutadores que proporcionan la conectividad con el exterior, una red troncal (normalmente Gigabit Ethernet) que se extiende por la estructura del edificio, un gran concentrador por planta que distribuye el tráfico desde la red troncal y luego varios concentradores más pequeños que conformarán las diferentes redes departamentales.

El primer paso a estudiar es buscar los puntos de fallo que puedan provocar una caída total de la red.

El siguiente punto a estudiar es el cableado de la red, comenzando por la red troncal. La red troncal suele ser Ethernet Grueso en sistemas antiguos y Gigabit Ethernet en los sistemas más modernos.

El tercer punto a estudiar es la posibilidad de fallo de los concentradores que conectan la red troncal con los concentradores de los distintos departamentos o secciones dentro del edificio.

El cuarto punto son los concentradores que interconectan las redes locales departamentales con los concentradores conectados a la red troncal.

3.2.4.3 Acceso físico al sistema

El acceso físico al hardware sea este computadoras o dispositivos de red deberá ser restringido, teniendo en cuenta las necesidades de cada departamento o usuario.

Es importante controlar y reflejar siempre en los apuntes quien ha accedido al hardware, con qué motivo y las modificaciones físicas o lógicas que en su caso pueda haber realizado sobre este hardware.

Una de las medidas más eficaces contra los ataques tanto físicos como informáticos sobre todo este tipo de sistemas es la monitorización continua de los dispositivos mediante sistemas de monitorización basados en hardware o software.

Los administradores de la red y de los servidores deberán mantener bajo observación estos dispositivos mediante esta monitorización buscando fallos y deberá evaluarse en cada caso si el fallo ha sido fortuito o se ha debido a algún tipo de manipulación sobre el hardware o sobre el software de los dispositivos.

3.2.4.4 Ubicación del hardware

La localización física del hardware puede afectar enormemente a la seguridad física del sistema, pues un sistema donde las máquinas estén expuestas a la manipulación del usuario final o de supuestos intrusos será un sistema poco seguro.

Es aconsejable mantener los dispositivos de red y los servidores en un lugar centralizado, idealmente un centro de datos donde podamos

tener las medidas de seguridad física indicadas anteriormente y donde el control de acceso permita saber quién, cuándo y porqué ha accedido físicamente a alguno de los dispositivos.

El acceso a los armarios deberá estar controlado y se deberá crear una política de acceso a los armarios, donde se apuntará de alguna de las formas anteriormente indicadas cada acceso a los dispositivos de red y servidores alojados en el armario, la persona que ha accedido y las manipulaciones que en su caso pueda haber realizado.

3.2.4.5 Control de acceso del personal al hardware

El control de acceso al hardware se realizará preferiblemente mediante personal que verifique mediante algún tipo de identificación a las personas que tienen permiso para acceder al hardware o mediante dispositivos electrónicos (claves, sistemas biométricos) o físicos (puertas blindadas, cerraduras seguras, etc.) que permitan controlar quien tiene acceso al hardware y quién no.

Es muy útil en estos casos tener una política clara y concisa sobre quien, como, cuando y para que puede tener acceso al hardware. Estas normativas deberán ser conocidas por todo el personal con acceso al hardware y deberán estar plasmadas sobre papel para poder ser consultadas en caso de duda.

3.2.4.6 Sistema de control de hardware y su integridad

Los sistemas de control de las condiciones de trabajo del hardware suelen ir integradas en los racks o armarios que usemos para protegerlos, indicando normalmente una serie de parámetros como la temperatura de trabajo, la humedad relativa del ambiente dentro del rack o armario y otros parámetros.

Los sistemas UPS de cierta entidad suelen tener algún medio de La integridad del hardware debe ser vigilada normalmente mediante software, ya sea mediante software de monitorización o sistemas de gestión de redes basados en SNMP (es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.).

Por esto es muy interesante que nuestros dispositivos de red dispongan de funcionalidad SNMP suficiente para poder monitorizar la salud de los dispositivos y su estado.

3.2.4.7 Desastres a nivel de hardware

La seguridad contra incendios y otros desastres han sido tratadas a nivel estructural anteriormente, pero ahora hablaremos de la seguridad a nivel de hardware, que proporcionará un segundo nivel de protección física.

La implementación de los sistemas de seguridad contra incendios, inundaciones, terremotos y demás desastres naturales deberá ser más estricta cuantos más críticos sean los datos que debemos proteger.

Se debe mantener un equilibrio entre el presupuesto dedicado a la seguridad física para este tipo de eventos y las pérdidas que puedan darse si uno de estos eventos se produce. Estas pérdidas pueden ser económicas, en horas de trabajo o en la integridad de datos críticos como datos económicos, datos de clientes o proveedores y datos secretos referidos a la empresa o a nuestros clientes o proveedores.

3.2.4.8 Evacuación de hardware

Aunque no sea muy común es interesante estudiar la posibilidad de que el hardware deba ser evacuado del edificio por diversas razones.

Es posible que tengamos que mover nuestro sistema a otro edificio por razones corporativas o que debamos hacerlo por razones de fuerza mayor, como desastres naturales, incendios parciales o cualquier otra contingencia imaginable. Para proveer este tipo de evacuación deberemos crear un plan de evacuación del hardware que nos permita llevar los equipos críticos a otro edificio o departamento en un mínimo de tiempo y siguiendo un plan predeterminado que tenga en cuenta la importancia de cada sistema.

Deberemos tener en cuenta al realizar el estudio y el plan de evacuación la importancia de los equipos y sobre todo de los datos que albergan estos equipos, de forma que los equipos y datos más importantes sean evacuados primero, y los menos importantes puedan esperar. Se deberá plantear la necesidad de tener personal preparado para este cometido y la facilidad con que estos datos se pueden mover de un lugar a otro.

Lo principal normalmente en una empresa será evacuar los datos corporativos (datos de la empresa, datos de facturación y contabilidad, del personal que trabaja en la empresa, de los clientes y de los proveedores), que estarán en forma de discos duros, sistemas de almacenamiento NAS o cintas de backups.

3.2.4.9 Del personal con su interacción con el hardware

Deberá tenerse en cuenta cuando se estudie el entorno de trabajo del personal de la empresa la formación que este personal ha recibido sobre seguridad informática y física de los sistemas sobre los que debe trabajar o que están localizados en su entorno más cercano.

Es fundamental que los empleados tengan los conocimientos necesarios para mantener el entorno del hardware físicamente seguro, y para esto deberán crearse normas de acceso y de uso de los

dispositivos hardware que el empleado deba manipular, poniendo especial hincapié en la seguridad de los datos y de su propio trabajo.

Los administradores deben por tanto implicarse en crear las normas de seguridad física, haciendo notar las normas que puedan entorpecer su trabajo y la mejor forma de realizar las prácticas de administración sin afectar a la seguridad física del sistema.

Es muy aconsejable que todo acceso o modificación sobre el hardware quede reflejado de alguna forma para que pueda ser comprobado posteriormente en el supuesto de fallos o problemas de funcionamiento del sistema.

3.2.4.10 Monitorización del entorno

Se aconseja siempre la instalación de dispositivos de control de la temperatura y de la humedad del entorno. El factor más crítico en los datacenters y en los racks y armarios ignífugos suele ser la temperatura, siendo la humedad un factor secundario sólo a tener en cuenta en climas muy determinados donde la humedad pueda afectar a los equipos.

Para prevenir una excesiva temperatura en los centros de datos y en los racks y armarios lo fundamental es tener una correcta ventilación y en el caso de habitaciones que alberguen una gran cantidad de máquinas la instalación de aparatos de aire acondicionado. A mayor temperatura menor tiempo entre fallos para todos los dispositivos electrónicos, incluidos los ordenadores, los dispositivos de red y cualquier sistema que genere por sí mismo calor.

Este sistema puede ser un simple termómetro electrónico en la sala de computación o en los racks y armarios o un sistema de adquisición de datos conectado a un termómetro que pueda mandar datos de la

temperatura a un ordenador que nos permita realizar la monitorización.

Un ejemplo de un sistema de este tipo son los diversos aparatos que existen para su integración con el software Nagios y que nos permiten mediante plugins de Nagios la monitorización de la temperatura de cualquier sistema, avisándonos cuando supera los límites preestablecidos.

3.2.4.11 Cableado eléctrico

Debemos tener en cuenta como consultores en seguridad física el cableado eléctrico en dos vertientes principales, las dos relacionadas pero independientes.

La primera de ellas es el cableado que proporciona energía a nuestros sistemas computacionales y dispositivos de red (e incluso otro tipo de dispositivos como impresoras láser o faxes) y que deben de cumplir como mínimo las normas aplicables a este tipo de cableado según el país donde nos encontremos, normalmente el reglamento de baja tensión.

Por ejemplo hay que estudiar que los enchufes y clavijas donde se conectan los dispositivos cumplen con las normativas aplicables y que no existe peligro de que pueda saltar una chispa entre terminales.

Otro punto a estudiar es el diámetro y la calidad del cableado, un determinado sistema alimentado por un cableado y calculando a partir de ahí la sección y calidad del cable que debe instalarse.

Un correcto aislamiento de este cableado puede mitigar este problema en gran medida.

En caso de duda siempre podemos consultar a personal especializado que puede realizar mediciones de campo sobre los

cables e indicarnos si pueden producir algún tipo de alteración sobre nuestros sistemas.

3.2.4.12 Cableado de telefonía

Poco más que añadir sobre el cableado de telefonía.

Deberemos observar que el cableado tiene la calidad y está homologado según la normativa del país donde nos encontremos. Deberemos tener también en cuenta lo dicho en el apartado anterior y mantenerlo lejos del cableado eléctrico que transporte mucha potencia.

Por lo demás el cableado de telefonía no suele dar ningún tipo de problemas, más que los puramente físicos como seccionamientos del cable, conectores mal montados o defectuosos y cosas así.

Es fundamental poder comprobar el cableado mediante aparatos fabricados a tal efecto de forma sencilla, para detectar roturas o seccionamientos del cable si tenemos el cable protegido por algún tipo de entubado o integrado en la estructura del edificio.

3.2.4.13 Cableado de redes

El cableado de redes es más sensible a las perturbaciones electromagnéticas que el cableado de telefonía, por transportar datos a una mayor frecuencia. Asumimos que estamos hablando de cable tipo ethernet del comúnmente instalado hoy en día.

Un caso diferente sería el antiguo cableado coaxial, que se recomienda sustituir por el nuevo cableado ethernet o el cableado de fibra óptica, que no sufre perturbaciones electromagnéticas y que tiene como único punto débil a estudiar su fragilidad, que no permite determinadas instalaciones, así como la mayor complejidad de sus conectores.

Es importante que todo el cableado y los conectores estén homologados, cumplan con la normativa aplicable y sean de la máxima calidad, a día de hoy CAT5 o CAT7.

3.2.4.14 Sistemas distribuidos

Cuando tenemos un sistema informático distribuido dentro del edificio debemos tener en cuenta que el factor más importante que debemos estudiar es la conectividad entre los distintos nodos, lo que implicará un estudio de la red pública (dentro del edificio) o privada que usen para comunicarse, así como los dispositivos de red que usen para su comunicación.

Deberemos realizar un estudio de la seguridad física de cada nodo y de cómo puede afectar la caída de uno de estos nodos al sistema distribuido, observando si la caída de un nodo provoca la caída del sistema, y entonces buscaremos algún tipo de alta disponibilidad o redundancia en los nodos, o si el sistema puede funcionar con algunos nodos caídos, con lo que el mismo sistema distribuido estará proporcionando la redundancia.

3.2.4.15 Llaves, cerraduras y armarios

La seguridad física de los armarios y racks es básicamente la de sus cerraduras y llaves, pues aunque podemos estudiar la fortaleza física del armario es poco probable que un supuesto atacante se ponga a reventar un armario o rack para acceder a su interior. Sobre todo cuando tiene otros métodos para hacerlo...

Las llaves y cerraduras dan una falsa seguridad al administrador de sistemas. La gran mayoría de los armarios y racks que se comercializan tienen cerraduras y llaves muy simples que pueden ser abiertas por cualquiera con un poco de habilidad y el material y los conocimientos necesarios.

La única solución es el adquirir armarios y racks con cerraduras seguras, que tengan al menos tres cilindros o que tengan cerraduras similares a las de las puertas blindadas. Solo esto nos asegurará que ningún intruso podrá acceder a nuestros dispositivos.

3.2.4.16 Cámaras de seguridad y monitorización

Las cámaras de seguridad son un elemento imprescindible si tenemos a nuestro cargo sistemas realmente críticos o sistemas especialmente atractivos para los supuestos intrusos o hackers.

Esto incluye todos los sistemas que alberguen datos económicos, números de tarjetas de crédito, datos de clientes o proveedores, datos personales de nuestros clientes, etc. Si tenemos centros de datos que almacenan datos de este tipo o cualquier tipo de datos críticos para el funcionamiento de la empresa o secretos deberemos tener personal de vigilancia contratado.

Lo ideal es tener personal de vigilancia presencial en el centro de datos para el control de acceso y luego personal de vigilancia encargado de la monitorización de las cámaras de vigilancia.

3.2.4.17 Control de ventanas y visibilidad desde el exterior

Uno de los errores en seguridad física más comunes que se suelen observar en entornos reales es la visibilidad desde el exterior de los monitores y teclados de los usuarios que están trabajando dentro del edificio.

Esto es un fallo de seguridad física muy importante, pues un intruso malintencionado puede observar desde una ventana o desde el exterior del edificio como el personal teclea sus passwords personales o datos secretos o críticos para la empresa.

La solución es muy sencilla. Basta con elegir la localización de los monitores y teclados fuera del alcance de un supuesto observador exterior.

3.2.4.18 Control de desechos y basura

¿A quién puede importarle nuestra basura?

Pensemos solo por un momento lo que puede obtener un posible intruso del contenedor de basura de una empresa: Documentación secreta sin destruir, números y claves de empleado, números de la seguridad social, planos de la empresa o de la red, datos técnicos de la red y de los sistemas informáticos de la empresa, datos sobre los empleados y la estructura administrativa de la empresa, números de teléfono internos, datos sobre la jerarquía administrativa de la empresa, y así hasta el infinito. Datos, datos, datos.

Un posible intruso puede usar todos estos datos para realizar todo tipo de hacking social sobre sus empleados y departamentos, usándolos para identificarse mediante llamadas a teléfonos internos y solicitar datos que normalmente no se darían si no fuera porque el interlocutor nos está dando datos que no debería saber si no trabajara en la empresa.

Este tipo de ataques de hacking social son cada vez más comunes y deben ser una preocupación principal para un consultor de seguridad física. Todos los documentos internos de la empresa deben de ser destruidos mediante máquinas que existen para esta tarea. Debe elegirse máquinas que destruyan totalmente los documentos, nada de tiras gruesas de papel que pueden volver a unirse con suficiente paciencia, cuanto más destruidos queden los documentos mejor.

La incineración de los documentos es por supuesto la opción ideal. Además debe de crearse una política de destrucción de

documentación que todos los empleados deberán cumplir, responsabilizándose cada uno de los datos y documentación que desechen.

3.2.5 Seguridad del hardware

La seguridad física del hardware es el último punto a estudiar por un consultor de seguridad física. Puesto que aquí no podemos confiar plenamente en el cumplimiento de políticas o normativas de uso de las máquinas y como estas máquinas están más expuestas a intrusos ajenos al personal de la empresa que hayan superado los controles de acceso de niveles superiores debemos configurar estas máquinas y dispositivos de red de forma que sea lo más complicado posible el realizar manipulaciones sobre ellos, tanto a nivel físico como a nivel informático siempre que sea posible. [Hall, 1996].

3.2.5.1 Acceso físico a las máquinas y dispositivos de red

Es inevitable que el personal tenga acceso físico a las máquinas sobre las que deben trabajar, y en algunos casos incluso a los dispositivos de red.

Los usuarios podrán acceder a sus datos a través de la red local y mantener los datos importantes a salvo, aunque el hardware donde van a trabajar este desprotegido por estar en su puesto de trabajo. Los sistemas NAS y otros sistemas de almacenamiento de datos o servidores de aplicaciones pueden ayudar en esto.

Por tanto la idea es mantener al menos los datos y el trabajo del usuario fuera de la máquina donde el usuario va a trabajar. Debemos instar al personal de administración para que organice el sistema de forma que los usuarios finales trabajen directamente sobre servidores de ficheros y servidores de aplicaciones, manteniendo así los datos a salvo de errores o manipulaciones del hardware.

3.2.5.2 Caja de la computadora

Las cajas de las computadoras suelen ser un dolor de cabeza para todo consultor de seguridad física, porque nos vienen impuestas por el hardware que se ha adquirido y es difícil el convencer a una empresa de que las cambie por otras más seguras.

La caja normal de una computadora no provee ningún tipo de seguridad contra un supuesto acceso a su interior por un intruso, todo lo contrario, cada vez se hacen más fáciles de abrir... Hay varias soluciones que se pueden aplicar para mejorar la seguridad de estos sistemas.

La primera y más simple sería el sellado de la caja, que al menos nos alertará si algún intruso ha accedido a su interior. Deberá instruirse al personal de mantenimiento para que ponga y quite los sellos cuando tengan que realizar algún tipo de manipulación dentro de la caja.

Otra solución es el taladrar y poner un candado o sistema similar en la caja que impida su apertura, aunque esto es difícil, puesto que lo que suele buscar un supuesto intruso son los datos contenidos en el disco duro, y para eso con abrir parcialmente la caja le basta.

La opción correcta es mantener estos datos en lugar seguro (un servidor de archivos dentro de un armario o rack) y que el usuario trabaje de forma remota sobre estos datos, con lo que la seguridad física del ordenador del usuario final será poco importante.

3.2.5.3 Seguridad de la BIOS

La seguridad que proporciona el passwords de BIOS es una seguridad absolutamente ficticia. Muchos administradores confían ciegamente en la seguridad de los sistemas asegurados mediante passwords de

BIOS, sobre todo cuando se intenta impedir el arranque desde disquetera o desde CDROM. Esto es un grave error.

La seguridad que proporciona el password de BIOS es mínima si no tenemos una seguridad física suficiente sobre el sistema en cuestión. Si un intruso consigue abrir la caja del ordenador puede simplemente activar el puente de borrado de la BIOS y nuestro password se borrará, o puede simplemente llevar un BIOS igual al del ordenador en cuestión y montarlo en el zócalo. Incluso se han dado casos de llegar a desoldar el BIOS de un ordenador y soldar el nuevo para saltar el password.

Por todas estas técnicas y por muchas otras que existen simplemente no debemos confiar en los password de BIOS. Si alguien tiene acceso al interior de nuestra máquina podrá hacer lo que quiera con ella. Puede borrar el BIOS, cambiarlo por otro, instalar una disquetera o un CDROM, una grabadora de CD, cualquier cosa. La seguridad física de la caja por tanto es fundamental si queremos asegurar que la configuración de la máquina no va a ser cambiada.

No nos cansamos de decirlo. Si tiene datos importantes manténgalos alejados de las máquinas de usuario o de cualquier máquina a la que pueda tener acceso un intruso malintencionado. Es la única forma de mantener sus datos a salvo.

3.2.5.4 Equipamiento hardware de las máquinas

Habiendo comentado ya el problema que existe con la poca seguridad que proporciona el BIOS de los ordenadores el equipamiento hardware que implementemos en la máquina no va a proporcionarnos más seguridad.

No vale que no instalemos disquetera ni CDROM ni grabadora de CD, y que deshabilitemos en el BIOS la detección de estos.

Si alguien tiene acceso físico al interior de la caja del ordenador siempre podrá cambiar el BIOS y luego instalar su propia disquetera, CDROM o grabadora de CD, por no hablar del acceso directo al disco duro, que puede sacar, clonar con herramientas como Norton Ghost y luego volver a dejar en su sitio sin que nadie se dé cuenta de que se ha replicado la información de la máquina.

3.2.5.5 Acceso al interior de los equipos

Hemos tratado ya el acceso al interior de las cajas de los ordenadores, que es un tema complicado. Más complicado aún es el acceso a los equipos de red, sistemas servidores de archivos, sistemas NAS, sistemas servidores de aplicaciones y similares.

La repercusión sobre la seguridad de la apertura de un NAS (Servidor de Almacenamiento) puede ser desastrosa. Todos los datos de trabajo de la empresa pueden quedar a disposición de un intruso. Muchos de estos sistemas tienen discos duros estándar, que pueden ser replicados con un portátil mediante Norton Ghost o similares y devueltos al sistema NAS sin que nadie detecte lo que ha ocurrido.

Insistimos. Lo único que nos salvará de este tipo de ataques de fuerza bruta (nunca mejor dicho) es el mantener este tipo de máquinas críticas protegidas en racks cerrados, en armarios bajo llave o en centros de datos con control de acceso. No hay más magia que esta, no busque soluciones esotéricas a problemas ya solucionados.

3.2.5.6 Control de calidad de las máquinas y dispositivos de red

El control de calidad de las máquinas y los dispositivos de red debe estar basado en dos premisas. La primera es la adquisición de equipos certificados y donde el fabricante nos asegure que se han realizado las pruebas de estrés suficientes sobre ellos para garantizar su calidad. La

segunda es la monitorización de estos equipos y la estimación de la vida útil y el tiempo medio de fallos en los mismos.

La adquisición de los servidores, los equipos de usuario final y los dispositivos de red dentro de una empresa debe estar regida en primer lugar por la calidad de estos.

Para ordenadores elegiremos máquinas de fabricantes que entreguen equipos completos pre configurado y probado en la cadena de montaje, es fundamental.

Las máquinas servidoras que se han de montar en rack suelen venir con certificación de su funcionamiento, así que sólo deberemos preocuparnos de las características de estas y de elegir un fabricante que distribuya los equipos pre configurados y probados en la cadena de montaje.

Los dispositivos de red deben ser elegidos entre los principales fabricantes de estos dispositivos. Elegir los dispositivos entre los grandes fabricantes nos asegurará que estos dispositivos han sido probados tanto en la fábrica como en miles de instalaciones reales hasta la saciedad, y nos permitirá solucionar los problemas que podamos tener con ellos fácilmente, pues existe una comunidad muy amplia de usuarios que pueden ayudarnos a través de las news o las listas de correo y permitirá al personal de mantenimiento mantener los equipos más fácilmente.

En general podemos concluir que la calidad de las máquinas y dispositivos de red son directamente proporcionales a su precio.

3.2.5.7 Control y seguridad de portátiles

Para el consultor de seguridad física los portátiles no suelen ser un gran problema, al menos no mayor que cualquier otra máquina del

sistema, pero para la seguridad informática los portátiles son un verdadero dolor de cabeza.

Comenzamos con la seguridad física. Debemos tener en cuenta la portabilidad de estos dispositivos, lo que los hace susceptibles de ser robados con facilidad, sobre todo cuando se encuentran fuera de la empresa.

En caso de robo el usuario debe comunicar con absoluta inmediatez a la empresa el evento que se ha producido, para que esta pueda minimizar los riesgos que implica el robo de los datos que ese portátil pueda contener.

Como regla general los portátiles que deban abandonar la empresa no deberían contener ningún tipo de dato importante o comprometido para la empresa. Si el usuario debe de usar estos dispositivos en otras empresas o en trabajos de campo deberán protegerse de todas las formas posibles los datos críticos que puedan contener, encriptándolos con sistemas seguros y permitiendo sólo el acceso al trabajador por medio de claves intransferibles de las que este deberá ser responsable.

La única solución, le responsabilizarían, de forma seria al usuario, y la integridad física de la máquina, teniendo una política muy clara de lo que el usuario puede hacer o no hacer con el ordenador.

3.2.5.8 Concentradores, bocas de red y conectividad

Los concentradores y las bocas de red suponen un peligro inmediato de seguridad física, pues cualquier intruso con un portátil o un aparato de mano con una tarjeta compactflash de red pueden conectar a cualquiera de ellas y probablemente obtendrá una dirección IP y conexión a la red interna de la empresa.

Para el caso de los concentradores el mantra es el mismo de siempre, deben estar en armarios o racks cerrados donde solo los

administradores de red tengan acceso a ellos. Para las bocas de red es más complicado.

Si tenemos que instalar una nueva máquina o necesitamos otra boca de red vamos al rack y conectamos el cable que da conectividad a la boca de red en cuestión. Tener todas las bocas de red conectadas es tener accesos libres a la red repartidos por toda la empresa que cualquiera puede usar, incluido un supuesto intruso.

3.2.5.9 Grabación de datos, grabadores de cd, disqueteras

No nos extenderemos excesivamente en este punto. Si su empresa necesita que los usuarios no se lleven datos de su empresa no los mantenga en la máquina del usuario.

Así de simple. El consejo que un consultor en seguridad puede darle no es otro más que el que mantenga los datos en los servidores y que los usuarios trabajen sobre los datos de forma remota.

Todos los demás sistemas son útiles pero no eficaces. Por eso lo mejor que puede hacer es no fiarse de ninguno de estos sistemas, simplemente mantenga los datos alejados del usuario final y así evitará que este pueda replicarlos.

3.2.5.10 Dongles usb y sistemas de almacenamiento usb.

Los dongles USB son como un dolor de muelas para los administradores de sistemas y los encargados de la seguridad del sistema. Para empezar tenemos lo que puede venir en ellos: virus, software pirateado, todo tipo de software o datos poco recomendables para un lugar de trabajo, juegos, etc. Luego tenemos todo lo que se puede llevar en ellos: datos de la empresa, software cuya licencia ha sido adquirido por la empresa, software bajado de internet, etc.

Si lo que más nos preocupa (tenemos antivirus, firewall, control de software, etc.) es que el usuario pueda replicar datos y sacarlos de la

empresa solo podemos hacer dos cosas, la primera y la que siempre recomendamos es mantener los datos lejos del usuario, la segunda es inhabilitar los puertos USB y los sistemas serie o paralelo, ya sea mediante métodos software o hardware.

La solución más radical (y no por ello la más recomendable) es quitar el cableado de los puertos USB frontales que conectan a la placa base y ya puestos a cacharrear podemos incluso sellar o desoldar los puertos USB integrados en la placa base.

3.2.5.11 Sistemas de radio frecuencia. Tecnología Wireless y bluetooth.

Existen 3 tipos de seguridad de wifi que son:

WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access)
WPA2 (Wi-Fi Protected Access)

La seguridad WEP es la que traen las redes wifi por defecto por lo menos en su mayoría, WPA mejora el sistema de cifrado que utiliza WEP aunque realmente es lo mismo en esencia pero mejora un poco el sistema de cifrado y por ultimo WPA2 presenta nuevas prestaciones que complican aún más el ataque, como la generación de claves dinámicamente cada cierto tiempo

Si me pregunta como consultor de seguridad física que puede hacer para mejorar su sistema de red mediante radiofrecuencia, sea este Wireless o Bluetooth mi primera respuesta será: ¡Quítelo ya!

Con los últimos sistemas lanzados y el nuevo WEP la seguridad ha mejorado, pero hace nada han salido varios bugs que permiten engañar a los sistemas Bluetooth y pueden estar seguros de que aparecerán otros bugs y formas de saltarse la seguridad de estos sistemas.

Son sistemas demasiado golosos para los hackers como para que estos no estudien mil y una formas de romperlos. Es muy cómodo ponerse con un coche y un portátil al lado de una empresa y

conectarse a la red de esta y realizar cualquier cosa como usar su ancho de banda para realizar ataques de denegación de servicio o Dios sabe qué. Mi consejo: Evítelas si puede.

3.2.5.12 Dispositivo de mano. Palms y pocketPcs.

Para los dispositivos de mano solo debemos decir que deben tomarse exactamente las mismas medidas que para los portátiles, aunque teniendo en cuenta que normalmente no contienen datos tan críticos para la empresa como los portátiles, aunque son mucho más fáciles de robar.

Es bastante común este caso, el robo de un dispositivo de mano con todos los datos de un empleado, que luego pueden ser usados para realizar hacking social, pues suelen contener números de teléfono internos de la empresa, datos sobre la empresa y en los casos más aterradores incluso passwords de acceso a los sistemas.

Lo mejor que se puede hacer es aconsejar a los empleados el no mantener nunca datos importantes en este tipo de dispositivos, sobre todo passwords de acceso, y el aconsejar también que si uno de estos dispositivos es robado o perdido se realice un informe para el empresa donde se indique al personal de seguridad que datos susceptibles de ser usados para hacking social o informático pudiera contener el dispositivo.

3.2.5.13 Control de acceso del personal externo contratado al hardware.

¿Cómo nos aseguramos que únicamente va a realizar las manipulaciones para las que le hemos contratado y no otras? Es sencillo, lo único que debemos hacer es tener un formulario que el personal externo deberá firmar y donde se especificará la fecha de la manipulación, la manipulación exacta que se le permite hacer y si es necesario también lo que no se le permite hacer. De esta forma

aseguramos que la persona que trabaje sobre nuestros sistemas no va a realizar más manipulación que la contratada.

3.3 Seguridad Lógica

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

La “seguridad lógica” involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.[José, 1997]

3.3.1 Objetivos de la seguridad lógica

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

3.3.2 Controles de acceso

Los controles de acceso pueden implementarse a nivel de Sistema operativo, de sistemas de información, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Estos controles constituyen una ayuda importante para proteger al sistema operativo de la red, a los sistemas de información y software adicional; de que puedan ser utilizadas(os) o modificadas(os) sin autorización; también para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con autorización de acceso) y para resguardar la información confidencial de accesos no autorizados.

3.3.2.1 Identificación y autenticación

Se constituye en la primera línea de defensa para la mayoría de los sistemas computarizados, al prevenir el ingreso de personas no autorizadas y es la base para casi todos los controles de acceso, además permite efectuar un seguimiento de las actividades de los usuarios. Identificación es cuando el usuario se da a conocer en el sistema; y Autenticación es la verificación que realiza el sistema de la identificación.

3.3.2.2 Roles

El acceso a la información puede ser controlado también, considerando la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: Líder de proyecto, Programador, Operador, Jefe de un área usuaria, Etc. Los derechos de acceso se agrupan de acuerdo con un rol determinado y el uso de los recursos se restringe a las personas autorizadas a asumir dicho rol, cambiar de rol implicaría salir del sistema y reingresar.

3.3.2.3 Transacciones

Otra planteamiento para implementar controles de acceso en una organización son las transacciones, sería del modo siguiente: el

computador conoce de antemano el número de cuenta que proporciona a un usuario el acceso a la cuenta respectiva, este acceso tiene la duración de una transacción, cuando esta es completada entonces la autorización de acceso termina, esto significa que el usuario no tiene más oportunidad de operar.

3.3.2.4 Limitaciones a los servicios

Las Limitaciones a los Servicios son controles que se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o que han sido preestablecidos por el administrador del sistema.

Un ejemplo de este tipo de control es: cuando en un cajero automático establece un límite para la cantidad de dinero que se puede transferir de una cuenta a otra, y también para los retiros.

3.3.2.5 Modalidad de acceso

El concepto de modo de acceso es fundamental para el control respectivo, los modos de acceso que pueden ser usados son: Lectura, Escritura, Ejecución, Borrado. Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación: Creación, Búsqueda.

Estos criterios pueden ser usados de manera conjunta con otros, por ejemplo, una organización puede proporcionar a un grupo de usuarios acceso de Escritura en una aplicación en cualquier momento dentro del horario de oficina, y acceso sólo de Lectura fuera de él.

3.3.2.6 Ubicación y horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto al horario, el uso de parámetros como horario de oficina o día de semana

son comunes cuando se implementan este tipo de controles, que permiten limitar el acceso de los usuarios a determinadas horas.

3.3.2.7 Control de acceso interno

Los controles de acceso interno determinan lo que un usuario (o grupo de usuarios) puede o no hacer con los recursos del sistema. Se detallarán cinco métodos de control de acceso interno:

3.3.2.7.1 Palabras claves

Las palabras clave o passwords, están comúnmente asociadas con la autenticación del usuario, pero también son usadas para proteger datos, aplicaciones e incluso PC's. Por ejemplo, una aplicación de contabilidad puede solicitar al usuario un password, en caso de que aquel desee acceder a cierta información financiera.

Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo e incluyen una gran variedad de aplicaciones.

3.3.2.7.2 Encriptación

La información encriptada solamente puede ser descryptada por quienes posean la clave apropiada. La criptología es un tema cuya amplitud será tratada en un subcapítulo aparte.

3.3.2.7.3 Listas de control de acceso

Estas listas se refieren a un registro de:

- Usuarios (incluye grupos de usuarios, computadoras, procesos), a quienes se les ha proporcionado autorización para usar un recurso del sistema.
- Los tipos de acceso que han sido proporcionados.

3.3.2.7.4 Límites sobre la interface de usuario

Comúnmente utilizados en conjunto con listas de control de accesos, estos límites restringen a los usuarios a funciones específicas.

Menús Vistas sobre la Base de Datos Límites físicos sobre la interface de usuario.

Las vistas sobre la Base de datos, limitan el acceso de los usuarios a los datos contenidos en la BD, de tal forma que los usuarios dispongan sólo de aquellos que puedan requerir para cumplir con sus funciones en la organización.

3.3.2.7.5 Etiqueta de seguridad

Las Etiquetas de Seguridad son denominaciones que se dan a los recursos (puede ser un archivo), las etiquetas pueden utilizarse para varios propósitos, por ejemplo:

Control de accesos, especificación de pruebas de protección, etc.

Las etiquetas de seguridad son una forma muy efectiva de control de acceso, pero a veces resultan inflexibles y pueden ser costosas de administrar, y estos factores pueden desanimar en su uso.

3.3.2.8 Control de acceso externo

Los controles de acceso externo son una protección contra la interacción de nuestro sistema con los sistemas, servicios y gente externa a la organización.

3.3.2.8.1 Dispositivo de control de puertos

Estos dispositivos autorizan el acceso a un puerto determinado del computador host y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem. Los dispositivos de control de puertos actúan de manera previa e

independiente de las funciones de control de acceso propias del computador y comúnmente son usados en comunicaciones seriales.

3.3.2.8.2 Firewalls o puertas de seguridad

Los firewalls permiten bloquear o filtrar el acceso entre 2 redes, generalmente una privada y otra externa (por ejemplo Internet), entendiendo como red privada una 'separada' de otras.

3.4 Premisas Básicas de Seguridad

3.4.1 Integridad

Significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

Esta propiedad permite asegurar que no se ha falseado la información.

Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado.

De hecho el problema de la integridad no sólo se refiere a modificaciones *intencionadas*, sino también a *cambios accidentales* o no intencionados.

3.4.2 Confidencialidad

La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

3.4.3 Disponibilidad

Se entiende por disponibilidad:

- El grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.
- La situación que se produce cuando se puede acceder a un SSI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.

3.4.4 No repudio

El no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

3.4.5 Autenticación

Autenticación es la verificación de la identidad del usuario, generalmente cuando ingresamos al sistema o a la red o accedemos una base de datos.

Es posible autenticarse, básicamente, de tres maneras:

- Por lo que uno sabe (una contraseña)
- Por lo que uno tiene (una tarjeta magnética)
- Por lo que uno es (huellas digitales)

La utilización de más de un método a la vez aumenta la seguridad de que la autenticación sea correcta.

3.4.6 Autorización

Es el proceso de determinar que, como y cuando, un usuario autenticado puede usar los recursos de la empresa.

Las autorizaciones pueden hacerse efectivas por medio de una firma en el formulario o por medio del ingreso de una contraseña específica en el sistema, si es importante que pueda registrarla para ser comprobada posteriormente. A nivel de datos, las autorizaciones son instrumentadas de manera de asegurar la confidencialidad e integridad, así sea otorgando o denegando el acceso a la posibilidad de leer, modificar, crear o borrar los mismos.

3.4.7 Trazabilidad

Toda acción pueda ser reproducida

3.4.8 Privacidad

Garantiza que los datos se respeten

3.5 Principios universales de la seguridad

Existen una serie de principios básicos que es necesario tener en cuenta al diseñar cualquier política de seguridad, nombramos algunos de ellos:

3.5.1 Principio de menor privilegio

Este es quizás el principio más fundamental de la seguridad, y no solamente de la informática.

Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener tan solo los privilegios de uso necesarios para desarrollar su tarea y ninguno más.

Esto quiere decir que cualquier usuario tan solo debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

3.5.2 La seguridad no se obtiene a través de la oscuridad

Un sistema no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corriamos estableciendo las medidas de seguridad adecuadas. El hecho de mantener posibles errores o vulnerabilidades en secreto no evita que existan, y de hecho evita que se corrija.

No se consigue proteger un sistema evitando el acceso de los usuarios a la información relacionada con la seguridad.

Por ejemplo, evitando el acceso a determinados manuales donde se especifican las ordenes que pueden utilizarse para entrar en el sistema. Educar a los usuarios o diseñadores sobre el funcionamiento del sistema y las medidas de seguridad incluidas, suele ser mejor método para protegerlo.

3.5.3 Principio del eslabón más débil

En todo sistema de seguridad, el máximo grado de seguridad es aquel que tiene su eslabón más débil. Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

Cuando diseñemos una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas. No basta con establecer unos mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.

3.5.4 Defensa en profundidad

La seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte que este sea, sino que es necesario establecer varios mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

Por ejemplo, en nuestro sistema podemos establecer un mecanismo de passwords altamente seguro como primera barrera de seguridad. Adicionalmente podemos utilizar algún método criptográfico fuerte para cifrar la información almacenada.

3.5.5 Punto de control centralizado

Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.

3.5.6 Seguridad en caso de fallo

Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro. Por ejemplo, si nuestros mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario que dejen pasar a cualquiera aunque no esté autorizado.

Quizás algunos ejemplos de la vida real nos ayuden más a aclarar este concepto. Normalmente cuando hay un corte de fluido eléctrico los ascensores están preparados para bloquearse mediante algún sistema de agarre, mientras que las puertas automáticas están diseñadas para poder abrirse y no quedar bloqueadas.

3.5.7 Participación universal

Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa, de los usuarios del sistema. Prácticamente cualquier mecanismo de seguridad que establezcamos puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo. La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.

3.5.8 Simplicidad

La simplicidad es un principio de seguridad por dos razones.

En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro.

En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

3.6 Políticas y Mecanismos

Una política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

3.6.1 Propósito de la política

El propósito de la política de seguridad de la información es proteger la información y los activos del banco de datos.

Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

3.6.2 Etapas en el desarrollo de una política

Hay 11 etapas que deben realizarse a través de la vida de una política, y están agrupadas en 4 fases:

3.6.2.1 Fase de desarrollo

Durante esta fase la política es creada, revisada y aprobada

a. Creación: planificación, investigación, documentación y coordinación de la política

El primer paso de la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política, o tomado todo junto, la creación. La creación de una política implica identificar por qué se necesita la política

Por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales.

Determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación.

La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir que autoridades deben aprobarlas, con quien se debe coordinar el desarrollo y estándares del formato de redacción) y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales.

b. Revisión: evaluación independiente de la política

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o individuo) independiente para su evaluación antes de su aprobación final.

Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de incremento en el número de involucrados; aumento de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión.

c. Aprobación: obtener la aprobación de la política por parte de las directivas

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de la aprobación, que coordine con dichos funcionarios, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración.

3.6.2.2 Fase de implementación

En esta fase la política es comunicado y acatada (o no cumplida)

a. Comunicación: difundir la política

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación.

La comunicación de la política es la primera etapa que se realiza en esta fase.

La política inicialmente debe ser difundida a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de ciertos servicios, etc.)

b. Cumplimiento: implementar la política

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras persona (del entorno) para interpretar cual es la mejor manera para implementar la política en diversas situaciones y oficinas; asegurando que las políticas sean entendidos por ellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas.

c. Excepciones: gestionar las situaciones donde la implementación no es disponible

Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través de periodo de tiempo establecido para la excepción.

El proceso también debe permitir excepciones permanentes a la política al igual que a la no aplicación temporal por circunstancias de corta duración.

3.6.2.3 Fase de mantenimiento

Los usuarios deben ser conscientes de la importancia de la política su cumplimiento debe ser monitorearlo, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

a. Concienciación: garantizar la concienciación continuada de la política

La etapa de la concienciación de la fase de mantenimiento comprende los esfuerzos continuo realizados para garantizar que las personas estén conscientes de la política y buscan facilitar su cumplimiento.

La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento.

La tarea final es medir la concienciación de los directivos con la política y ajustar los esfuerzos de acuerdo con los resultados de las actividades medidas.

b. Monitoreo: seguimiento y reporte del cumplimiento de la política

Esta información se obtiene de la observación de los supervisores, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes.

Esta etapa contiene actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

c. Garantía de cumplimiento: afrontar las contravenciones de la política

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir.

Se recomienda incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

d. Mantenimiento: asegurar que la política este actualizada

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política.

Esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etc.) que pueda afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio.

3.6.2.4 Fase de eliminación

La política se retira cuando no se requiera más

a. Retiro: prescindir de la política cuando no se necesita más.

Después que la política ha cumplido su con su finalidad y no es necesaria (por ejemplo: la empresa cambio la tecnología a la cual aplicaba o se creó una nueva política que la remplazo) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación de ciclo de vida de la política. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política.

3.6.3 Mecanismos de la seguridad

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático. [Facundo, 2010].

3.6.4 Clasificación según su función

3.6.4.1 Preventivos

Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.

3.6.4.2 Detectivos

Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

3.6.4.3 Correctivos

Actúan luego de ocurrido el hecho y su función es corregir la consecuencias.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles

3.6.4.4 Huella digital

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

3.6.4.5 Verificación de voz

La dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

3.6.4.6 Verificación de patrones oculares

Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

3.7 Documentación formal de la seguridad

3.7.1 Política

Declaración general de principios que presenta la posición de la administración para un área de control definida.

Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por la directiva, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias.

Las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción. **[Guido, 2002]. Ver Anexo 1.**

3.7.2 Estándar

Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas.

Los estándares sirven como especificaciones para la implantación de las políticas: son diseñadas para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas. **[Jule, 2010].**

3.7.2.1 Trusted Computer Security Evaluation Criteria. TCSEC.

El Departamento de Defensa de los Estados Unidos por los años 80's (1983-1985) publica una serie de documentos denominados Serie Arco iris (Rainbow Series). Dentro de esta serie se encuentra el Libro Naranja (Orange Book) el cual suministra especificaciones de seguridad.

Se definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 él más elevado. Todas las clases incluyen requisitos tanto de funcionalidad como de confianza.

- **Nivel D (Protección mínima)**

Sin seguridad, está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.

- **Nivel C1 (Protección Discrecional)**

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, debido a que no hay forma de distinguir entre los cambios que hizo cada usuario.

- **Nivel C2 (Protección de Acceso Controlado)**

Este nivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.

- **Nivel B1 (Seguridad Etiquetada)**

Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

- **Nivel B2 (Protección Estructurada)**

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

- **Nivel B3 (Dominios de seguridad)**

Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones.

- **Nivel A1 (Protección verificada)**

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

Por la década de los 90's se publicó Minimum Security Functionality Requirements (MSFR) por el National Institute of Standards and Technology (NIST). En 1992 se creó Federal Criteria

3.7.2.2 Information Technology Security Evaluation Criteria. ITSEC.

Por su parte el Information Technology Security Evaluation Criteria (ITSEC), conformado principalmente por Francia, Alemania y Reino Unido, crearon su propio estándar de seguridad, al principio de los 90's, este se conoce como el Libro Blanco (White Book).

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada. E1, el punto de entrada por debajo del cual no cabe la confianza útil, y E6 el nivel de confianza más elevado.

Por su parte Canadá en 1993 publicó Canadian Trusted Computer Product Evaluation Criteria (CTCPEC).

Estos documentos no satisfacían las exigencias de seguridad de los diversos países involucrados, por lo cual se creó un documento que unificará estos criterios dando origen a los Criterios Comunes.

3.7.2.3 ISO 15408 Criterios Comunes (CC)

Los CC (Criterios Comunes) su primer versión surgió en el 96, pero Europa paralelamente trabajó en un estándar ISO, esto nos regresaba al problema original, tener criterios diferentes de seguridad dependiendo del continente en el que se encontrará; para el año 2000 se unificaron criterios nuevamente dando lugar a un estándar internacional que puede ser conocido con el nombre de Common Criteria o ISO-15408.

En el año del 2005 se actualizaron los CC dando origen a CC versión 2.2 también conocido como ISO-15408:2005. Pero, ¿porque son tan importantes los CC en la Seguridad de la Información (SI)?

Los CC nos ofrecen una norma internacional para evaluar la seguridad de los productos de tecnología de la información. Se puede pensar en tres diferentes perspectivas desde las cuales los podemos abordar: Como consumidores proveen criterios que determinan las necesidades de seguridad que deben cumplir los productos que se deseen adquirir.

Como desarrolladores proveen criterios que permite cubrir requerimientos de seguridad en diferentes niveles. Como evaluadores proporcionan los productos de seguridad que deben ser cubiertos por los desarrolladores.

Los CC están divididos en 3 partes:

- Introducción y Modelo General.
- Requerimientos Funcionales.
- Requerimientos de Garantía.

A veces se tiene la idea de que no es bueno utilizar CC para implementar un esquema de seguridad, porque se piensa que no son certificables debido a que son muy generales. Por esta razón se usan estándares como pueden ser el ISO-17799 o el ISO-27000.

3.7.2.4 BS 7799 (Reino Unido)

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización inglesa equivalente a AENOR en España).

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

El estándar británico BS 7799 es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información incluyendo el ISO 17799.

La versión actual de estándar tiene dos partes:

- **BS7799-1:1999 Information Security Management. Code of Practice for Information Security Management.** Es la guía de buenas prácticas, para la que no se establece un modelo de certificación.
- **BS7799-2:1999 Information Security Management. Specification for Information Security Management Systems.** Establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

3.7.2.5 ISO 17799

El estándar de seguridad de la información ISO 17799, es descendiente del BS 7799 – Information Security Management

Standard – de la BSI (British Standard Institute) que publicó su primera versión en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

- **Parte 1.** Código de prácticas.
- **Parte 2.** Especificaciones del sistema de administración de seguridad de la información.

Por la necesidad generalizada de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS 7799 Part 1: Code of Practice).

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

- **Confidencialidad.** Asegurar que únicamente personal autorizado tenga acceso a la información.
- **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

3.7.2.6 Los controles del ISO 17799

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce en la jerga del estándar como Statement of Applicability, que es la definición de los controles que aplican a la organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

A continuación, se describirán cada una de las diez áreas de seguridad con el objeto de esclarecer los objetivos de estos controles.

1. Políticas de seguridad. El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

2. Seguridad organizacional. Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

3. Clasificación y control de activos. El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

4. Seguridad del personal. Proporcionar controles a las acciones del personal que opera con los activos de información.

El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

5. Seguridad física y de entorno. Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

6. Comunicaciones y administración de operaciones. Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

7. Control de acceso. Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

8. Desarrollo de sistemas y mantenimiento. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

9. Continuidad de las operaciones de la organización. El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

10. Requerimientos legales. La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

3.7.2.7 ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El ISO-27000 se basa en la segunda parte del estándar británico BS7799 (BS7799:2). Está compuesta a grandes rasgos por:

- ISMS (Information Security Management System).
- Valoración de Riesgo.
- Controles.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

- **ISO 27000:** En fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma será gratuita, a diferencia de las demás de la serie, que tendrán un coste.

- **ISO 27001:** Es la norma principal de requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.
- Enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.
- **ISO 27002:** Cambio de nomenclatura de ISO 17799:2005 realizada el 1 de julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- **ISO 27003:** En fase de desarrollo; probable publicación a finales de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- **ISO 27004:** En fase de desarrollo; probable publicación a lo largo de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

- **ISO 27005:** En fase de desarrollo; probable publicación a finales de 2007 ó principios de 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basará en la BS7799-3 (publicada en marzo de 2006) e ISO 13335-3.
- **ISO 27006:** Publicada en febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

3.7.3 Mejor practica

Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar un enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización. **[W.Stallings, 1995].**

3.7.4 Guía

Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo. **[Guido, 2002].**

3.7.5 Procedimientos

Los procedimientos definen específicamente como las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o

de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. **[Guido, 2002].**

Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados, implementados y supervisados por el dueño del proceso o sistema.

Los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

IV. CONCLUSIONES


- Debido al constante crecimiento de la tecnología a nivel mundial, el ataque y las amenazas hacia la seguridad informática son cada vez más frecuentes provocando que las organizaciones requieran implantar políticas, normas, procedimientos con el fin de reducir el impacto de las amenazas y ataques.
- Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.
- Mediante el internet podemos conocer muchos mecanismos de seguridad existentes en todo el mundo, podemos aplicar en nuestras vidas cotidianas lo cual nos servirá de mucha ayuda para una mejora continua.
- Utilizando las políticas, mecanismos, estándares y procedimientos establecidos por las organizaciones internacionales, podemos hacer que la seguridad informática dentro de las organizaciones funcione, y pueda evitar que personas ajenas afecten la organización.
- Mediante la lectura de este informe, podemos aprender la seguridad informática como usar, realizar y aplicar los procedimientos, mecanismos.

V. REFERENCIAS BIBLIOGRAFICAS

- Morant Ramos, J.L., Ribagorda Garnacho, A. y Sancho Rodríguez, J. Seguridad y Protección de la Información, 1ª edición, Ed. Centro de Estudios Ramón Areces, S.A. (CERASA), 1994.
- Stuart Tanenbaum A. Redes de Computadores. 3ª edición. Prentice Hall 1996
- Stallings, W. Comunicaciones y Redes de Computadores. 5ª edición Prentice Hall 1997.
- Russell, D. Gangemi, G.T. Seguridad Informática básica. O'Reilly, 2nd Edición 1996.
- Stallings, W. Red e Internet. Seguridad de la red. Principios y Práctica. 2nd Edición .Prentice Hall 1995
- Calle Guglieri, J. A .Reingeniería y seguridad en el espacio. Ediciones Diaz de Santos. 1997.
- Athanase Peltier, J.C. Políticas y procedimientos de seguridad de la información. Auerbach Publications. New york. 1999.
- Killmeyer, J. Arquitectura de seguridad de la información: un enfoque integrado de la seguridad en la organización. New York 2001.
- Ramió Aguirre, J. Seguridad Informática y Criptografía (Aplicaciones Criptográficas. Segunda Edición), Publicaciones EE.UU 1999.
- Maiwald, Eric. Fundamentos de seguridad de redes. Segunda Edición. México, McGraw Hill. 2005.
- Sanders, D., Informática presente y futuro. Editorial McGraw Hill, Mexico 2001
- Estándares [Acceso 18 de Diciembre del 2014] Disponible en : <http://www.iso.org/>
- Estándares [Acceso 18 de Diciembre del 2014] Disponible en : <http://www.iso27000.es/sgsi.html>

ANEXOS

ANEXO 1: POLITICA DE SEGURIDAD

	POLITICA DE SEGURIDAD INFORMATICA	
	SIMA IQUITOS S.R.LTDA. OFICINA ESTRATEGICA	Fecha: 10/08/2012 Páginas: 2

POLITICA DE SEGURIDAD INFORMATICA

Autor	Darwin TUESTA Valera
Cargo	Jefe de División de Planeamiento y Desarrollo
Fecha	10/08/2012

RESPONSABLES Y REVISIÓN DEL DOCUMENTO

HISTORIAL DE CAMBIOS

Fecha	Autor	Versión	Referencia de Cambio
10/08/2012	Darwin TUESTA	1.0	Creación del Documento

REVISION

Nombre	Versión Aprob.	Cargo	Fecha
Giovanni MIÑAN	1.0	Jefe Oficina Estratégica	10/08/2012

Elaborado por:	Revisado por:
Darwin TUESTA Valera Jefe División de Planeamiento y Desarrollo	Capitán de Fragata Giovanni MIÑAN Protto Jefe Oficina Estratégica

Se han definido las siguientes políticas de seguridad:

- El usuario es responsable de la seguridad e integridad de la información que maneja, lo cual protege mediante una palabra clave de acceso (password).
- Las contraseñas no deben ser iguales a los nombres o apellidos del usuario, pues resultaría fácil de descifrar y deben tener como mínimo 8 caracteres.
- Cambiar cada 30 días la clave de acceso, para evitar riesgos de descifrase.
- La clave de acceso (password), debe mantenerse en reserva, ya que ésta es de carácter personal, y deberá conocer solamente el usuario responsable del acceso.
- Evitar escribir el password en papeles sueltos, ya que se corre el riesgo de extraviarlos, y por consiguiente dar acceso a personas ajenas a la información, en caso de hacer esto se recomienda guardar la clave de acceso en lugar seguro o memorizarlo.
- En el momento de digitar su clave personal, procure tener la privacidad adecuada, que amerita el caso.
- En caso de no recordar la clave de acceso o pérdida de ésta, comunicar a la División de Tecnologías de la Información, para la asignación de un password nuevo.
- El acceso a la información se define como de carácter confidencial y no de conocimiento público, su manejo está restringido a personal autorizado de la empresa, y su uso indebido podría ser lesivo a los intereses de la empresa y comprometer a la persona, toda salida o ingreso de la información a la empresa es registrada en el **Registro de Entrada y/o Salida de información.**
- Evitar la manipulación de los equipos y/o programas informáticos a personas ajenas al área de trabajo.
- Evitar dejar encendido y con acceso a red, para ir almorzar, o salir a algún lugar por tiempo prolongado o indeterminado, es conveniente salir de red y apagar el equipo, para que no exista riesgo de manipulación de

su equipo y/o información; antes de apagar el equipo salir correctamente de todos los programas que se tengan en uso.

- La utilización de disquetera será autorizada por la Jefatura Simal.
- En caso que su computadora, disponga de una disquetera habilitada:
 - No deberá ingresar discos extraños al equipo.
 - No debe usarse con otro fin, al autorizado.
 - Llevar un registro de las copias y/o lecturas de los discos efectuados.
- Está prohibido fumar en las oficinas que tienen computadoras.
- Si se observa un correo electrónico de dudoso origen, informar inmediatamente al Jefe de la División de Tecnologías de la Información para su verificación.
- La privacidad de su cuenta de correo electrónico dependerá exclusivamente del dueño de esta.
- Está prohibido propagar mensajes que contienen contenidos impropios, financieros o de otros temas que son ajenos a su puesto de trabajo en la empresa.
- Si alguna terminal trabaja de manera sospechosa (velocidad anormal, mensajes extraños, etc.), se informara inmediatamente al Jefe de la División de Tecnologías de la Información para su verificación.
- Chequear semanalmente la presencia de virus informáticos, utilizando el programa de virus establecidos.
- Efectuar el Backup semanal de la información del área, el cual no se encuentra en los sistemas informáticos.
- Los jefes de cada Área deben verificar que el proceso de Backup se realice normalmente.
- Al terminar el día laborable deberá apagar correctamente el computador y dejarlo desconectado del servicio eléctrico.