POLÍTICA DE SEGURIDAD INFORMÁTICA Y APLICABILIDAD EN LA RED DE DATOS DE LA EMPRESA CELTEL S.A.

HENRY JAVIER BARON GONZALEZ
Ingeniero de Sistemas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2007

POLÍTICA DE SEGURIDAD INFORMÁTICA Y APLICABILIDAD EN LA RED DE DATOS DE LA EMPRESA CELTEL S.A.

HENRY JAVIER BARÓN GONZALEZ
Ingeniero de Sistemas

Monografía para obtener el titulo de
Especialista en Telecomunicaciones

Director del Proyecto:
M. Eng. SAMUEL GONZALO PINZÓN BARRIOS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2007

A Dios por darme la vida
y la familia tan maravillosa que tengo.
A mis padres y hermanos que me fortalecen con su cariño.
A Ángela y Sandra por su apoyo incondicional.

AGRADECIMIENTOS

Deseo expresar mis agradecimientos a:

La Universidad Industrial de Santander, institución que contribuyó significativamente a mejorar mi formación profesional.

A los docentes de la Especialización en Telecomunicaciones, por su espíritu investigativo y constante interés en mejorar la calidad del programa académico.

Al ingeniero Samuel Pinzón, por su dirección y colaboración en la realización de éste proyecto.

A mis compañeros de la especialización, por su amistad.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BACKUPS: Son diferentes medios donde residen las copias de seguridad.

BUGS*:* Son errores de programación cometidos de forma involuntaria por los programadores de sistemas de aplicaciones.

CONFIDENCIALIDAD: Garantiza que los objetos de un sistema van a ser accedidos únicamente por los elementos autorizados.

CRACKERS: Son aquellas personas que buscan molestar a otras personas, piratear software protegido por las leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus. Generalmente son adolescentes que aprenden rápidamente sistemas y no poseen ningún tipo de ideología cuando realizan sus trabajos.

DIALERS: programas de marcación telefónica de tarifa especial.

DIRECTRICES: Reglas generales de nivel estratégico donde se expresan los valores de una organización.

DISPONIBILIDAD: Los objetos de un sistema pueden ser accedidos en el momento que sean requeridos.

EXPLOITS*:* Son programas utilizados para aprovechar errores de programación y atacar al sistema.

HACKERS*:* Personas que con ayuda de sus conocimientos informáticos consiguen acceder a un sistema informático (bancos, empresas

prestigiosas), obtener cuentas de usuario validas, realizando rastreos de cuentas poco usadas o un punto débil del sistema de seguridad. Otra actividad que puede hacer el hackers es aprender a usar el sistema informático vulnerado. La mayoría de los hackers no destruyen ni dañan deliberadamente los datos.

INTEGRIDAD: Los objetos de un sistema sólo pueden ser modificados por los elementos autorizados.

LOGIN*:* Es un nombre o identificación del usuario en el sistema.

NORMAS*:* Reglas generales y específicas de tipo táctico, que pueden ser especificas para un público en particular.

POLÍTICA DE SEGURIDAD: Son reglas y procedimientos que regulan la forma de prevenir, proteger y manejar los riesgos en una organización.1

PROCEDIMIENTOS*:* Conjunto de pasos para realizar una actividad especifica.

SNIFFING: consistente en capturar tramas que circulan por la red mediante un programa ejecutándose en una máquina conectada a ella o bien mediante un dispositivo que se engancha directamente el cableado.

SPAM*:* correos electrónicos no deseados.

SPYWARE*:* aplicaciones que cogen datos de los ordenadores de los usuarios para después comercializarlos**.**

TITULO POLÍTICA DE SEGURIDAD INFORMÁTICA Y APLICABILIDAD EN LA RED DE DATOS DE LA EMPRESA CELTEL S.A.[*]

AUTOR BARON GONZALEZ HENRY JAVIER[**]

PALABRAS CLAVES: Vulnerabilidades, virus, intrusos, ataques informáticos, redes de datos, interrupción, interceptación, modificación, destrucción, seguridad informática, integridad, disponibilidad, confidencialidad, Políticas de Seguridad Informática.

DESCRIPCIÓN

En la actualidad, las diferentes organizaciones o empresas utilizan sus redes corporativas junto a la Internet, para el desarrollo de sus actividades económicas o comerciales, utilizando diferentes tecnologías para trasmitir grandes volúmenes de Información, que en su gran mayoría son de carácter confidencial; por ésta razón, la seguridad informática es un tema de gran importancia para los administradores de las redes de datos, puesto que deben garantizar la integridad, disponibilidad y confidencialidad de la información.

Los virus y los errores de programación cometidos en forma involuntaria por los desarrolladores de aplicaciones, han dejado de ser el principal problema para los administradores de redes de datos y las únicas amenazas informáticas serias que se deben afrontar; también se deben tener en cuenta las deficiencias en la seguridad de las redes de datos, puesto que facilitan el acceso a intrusos, que tienen como objetivo, sacar provecho de la información capturada, utilizando diferentes ataques como la interrupción, interceptación, modificación o destrucción.

El presente trabajo de monografía esta orientado a identificar las vulnerabilidades más comunes que presentan las empresas y realizar un estudio de riesgos a la empresa de Celulares y Telecomunicaciones CELTEL S.A., con el objetivo de diseñar un manual de políticas de seguridad informática, que permita administrar en forma adecuada los recursos de computo existentes, que asigne a todo el personal sus funciones y responsabilidades, ante la presencia de un incidente de seguridad y que sirva como herramienta para mejorar la gestión administrativa de la empresa.

[*] Monografía

[**] Facultad de Ingenierías Físico Mecánicas. Ingeniería Eléctrica, electrónica y de Telecomunicaciones. Especialización en Telecomunicaciones. M.Eng Samuel Gonzalo Pinzón Barrios.

TITLE COMPUTER SCIENCE SECURITY POLICY AND ITS APPLICABILICATIONS IN CELTEL S.A. COMPANY'S DATA NETWORK.[*]

AUTHOR: BARON GONZALEZ HENRY JAVIER[**]

KEY WORDS: Computer science vulnerabilities, virus, intruders, attacks, data networks, interruptions, interceptions, modifications, destruction, integrity, availability, confidentiality, computer science security policy.

DESCRIPTION

At the present time, different organizations or companies use their corporative networks alongside the Internet, for their economic development or commercial activities, using different types of technology to transmit large amounts of Information, within which there are a great number of confidential characters; for this one reason, the computer science security is a subject of great importance for the administrator of the data network, since they must guarantee integrity, availability and confidentiality of the information.

The virus and the committed errors and the programming in involuntary forms bye the application developers, have stopped being the main problem for the network administrator of data and to the only serious computer science threats that are due to confront, also the deficiencies in the security of the data network are due to consider, since they facilitate intruders in accessing the system, whom they have like objective to removal of information, using different methods, such as, interruptions, interceptions, modifications or destruction.

Monograph work is used to identify the most common vulnerabilities that are present within a company and conduct a study of risks to the cellular and telecommunications company, "CELTEL S.A.", with the objective of designing computer science security policy guide, which would allow administers compute existing resources, which assigned to all the personnel who are responsible for the functions during a security incident, and which serve as a tool to improve administrative management within the company.

[*] Monograph

[**] Physical Mechanical Engineerings Faculty. Electrical, Electronic and Telecommunications Engineerings. Telecommunication Specialization. M.Eng Samuel Gonzalo Pinzón Barrios.

INTRODUCCIÓN

La deficiencia de seguridad en las redes de datos, es un problema que a pesar de su importancia no ha recibido la atención necesaria, por parte de los administradores de redes o responsables del manejo de la información en las diferentes empresas a nivel nacional.

Los virus han dejado de ser el principal dolor de cabeza de los administradores de redes de datos y las únicas amenazas informáticas serias que las empresas y usuarios tienen que hacer frente. Los intrusos y atacantes de redes de datos han cobrado gran popularidad.

No existen sistemas totalmente seguros, que estén libres de intrusos, atacantes o cualquier tipo de daño o riesgo; pero existen sistemas fiables que garantizan el cumplimiento de tres aspectos muy importantes como son: la confidencialidad, disponibilidad e integridad.

Este trabajo es de gran utilidad para los administradores de redes informáticas, el personal encargado de la seguridad de la información, profesionales en sistemas y telecomunicaciones; porque permitirá tener un marco de referencia actualizado para identificar los ataques informáticos más utilizados y de igual forma plantea los pasos para diseñar la política de seguridad informática que debe ser implementada por la empresa CELTEL S.A., con el objetivo de reducir las posibilidades de ver la red de datos comprometida, ante los diferentes ataques informáticos existentes.

1. FUNDAMENTACIÓN TEÓRICA

1.1 ¿QUE ES SEGURIDAD INFORMÁTICA?

La seguridad informática es el resultado del vínculo estrecho que deben tener un conjunto de elementos como el hardware, el software, procedimientos y documentos, que permiten que un sistema informático se comporte tal como los usuarios esperan de él y que sus recursos disponibles sean accesados únicamente por quienes tengan la autorización de hacerlo.

Mantener un sistema seguro o fiable consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. La ***confidencialidad*** permite que los objetos de un sistema sean accedidos únicamente por elementos autorizados, y que esos elementos autorizados no van a permitir que esa información este disponible para otras entidades; la ***integridad*** significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la ***disponibilidad*** indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados. Generalmente tienen que existir los tres aspectos descritos para que un sistema sea fiable. .

Dependiendo del entorno, se da mayor prioridad a ciertos aspectos de la seguridad, que a otros. Por ejemplo, en un sistema militar se da mayor importancia a la confidencialidad de los datos almacenados o transmitidos, mientras que en una empresa comercial será primordial la disponibilidad o en un entorno bancario es más importante para los administradores del sistema, la integridad de los datos frente a la disponibilidad o la confidencialidad.

1.2 ¿QUÉ QUEREMOS PROTEGER?

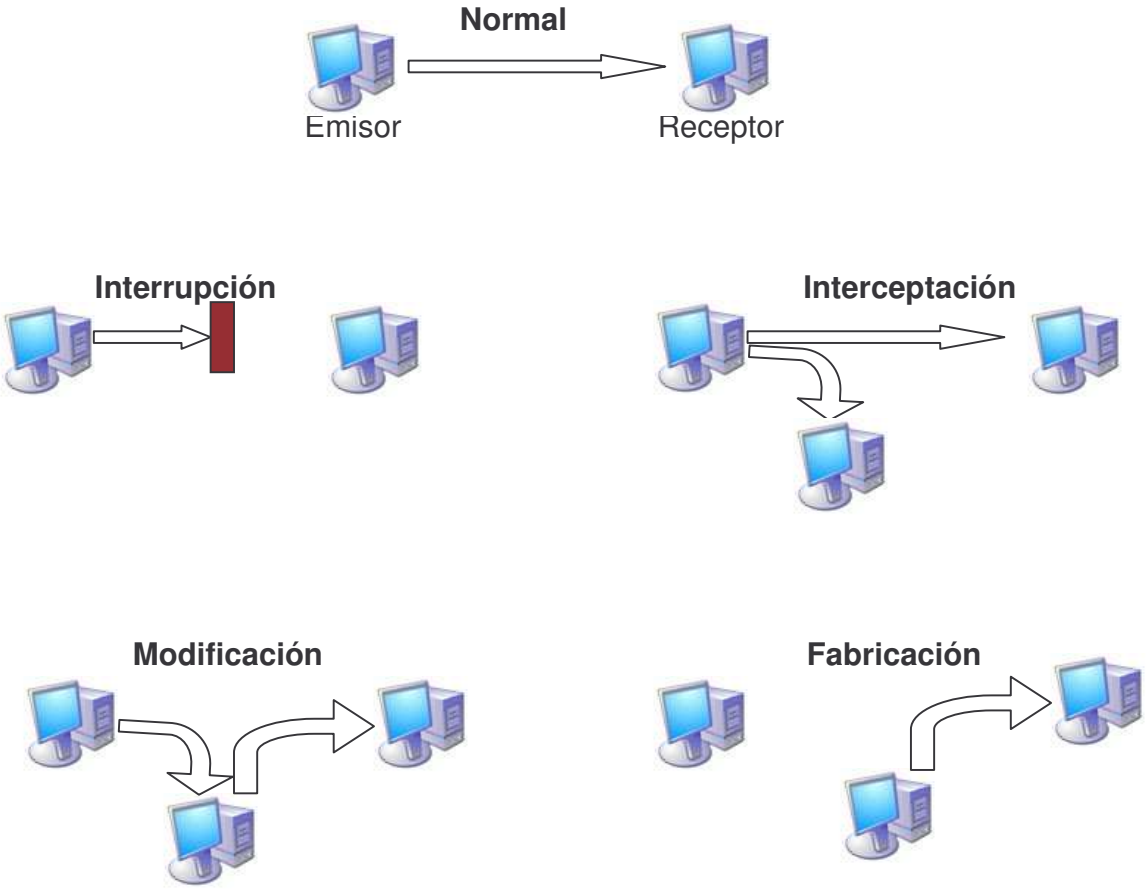
Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar: con toda seguridad los servidores están ubicados en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación o el propio sistema operativo, éste *software* se puede restaurar sin problemas desde su medio original (CD-ROM de instalación). Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio 'original' desde donde se pueda restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

Contra cualquiera de los tres elementos descritos anteriormente, pero principalmente sobre los datos se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Estas amenazas se dividen en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación.[1] Un ataque se clasifica como ***interrupción*** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una ***interceptación*** si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una ***modificación*** si además de conseguir el acceso, consigue modificar el objeto; se considera un caso especial de la modificación: la *destrucción*, entendiéndola como una

[1] Las siguientes secciones de éste capitulo, fueron tomadas principalmente de las direcciones electrónicas: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html a las cuales se les realizó las adecuaciones correspondientes para ser presentadas en la monografía, sin cambiar el contenido temático expuesto en la versión original. De igual manera al ser un documento público y no constar explícitamente los derechos de autor, el autor de la monografía no está incumpliendo las normas estatales en dicho tema.

modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una ***fabricación*** si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el "fabricado".

Figura 1 Flujo de la información entre el emisor y el receptor



1.2.1 Amenazas del Hardware

El *hardware* es uno de los elementos más caros de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización; teniendo en cuenta que las empresas poseen entre sus equipos máquinas muy costosas, como servidores de gran potencia de cálculo, *routers* de última tecnología o modernos sistemas de transmisión de datos como la fibra óptica, entre otros.

A continuación se describen algunas de las amenazas al *hardware*, sus posibles efectos y algunas soluciones, para minimizar el riesgo.

1.2.1.1 Acceso físico

La posibilidad de acceder físicamente al servidor, sin importar el sistema operativo que este instalado, hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre el. Si un atacante puede llegar con total libertad hasta una estación, puede por ejemplo abrir la CPU y llevarse un disco duro; sin necesidad de privilegios en el sistema, sin importar la robustez de nuestros cortafuegos, sin ni siquiera una clave de usuario, el atacante podrá seguramente modificar la información almacenada, destruirla o simplemente leerla.

Mientras que muchos de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento, otros estarán en lugares de acceso semipúblico, como las estaciones de trabajo en ciertas oficinas o equipos de servicio al cliente; es justamente sobre estos últimos, sobre los que se debe extremar las precauciones, ya que lo más fácil y discreto para un atacante es

acceder a uno de estos equipos y, en segundos, lanzar un ataque completo sobre la red.

1.2.1.2 Desastres naturales

En el anterior punto hemos hecho referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física; también existen:

- **Terremotos**

Es recomendable no situar nunca equipos delicados en superficies muy elevadas, aunque tampoco es bueno situarlos a ras de suelo. Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo *hardware*, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente utilizar fijaciones para los elementos más críticos, como la cpu, los monitores o los *routers*. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarán el *hardware*.

No debemos entender por terremotos únicamente a los grandes desastres que derrumban edificios y destrozan vías de comunicación; quizás sería más apropiado hablar incluso de *vibraciones*, desde las más grandes, los terremotos hasta las más pequeñas, un simple motor cercano a los equipos. Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos

utilizar plataformas de goma, para que éstas absorban la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con *hardware* más mecánico, como las impresoras; estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima de la CPU de una máquina es una mala idea.

- **Tormentas eléctricas**

Las tormentas con aparato eléctrico, generan subidas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica, como veremos a continuación. Si cae un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir *hardware* incluso protegido contra voltajes elevados. En caso de presentarse una tormenta muy fuerte, lo más conveniente es desconectar los equipos de cómputo.

Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, que se han de almacenar lo más alejados posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar todas las cintas o discos, lo que añade a los problemas por daños en el *hardware* la pérdida de toda la información del sistema.

- **Inundaciones y humedad**

Cierto grado de humedad es necesario para un correcto funcionamiento de las máquinas: en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que, como veremos más tarde, puede transformar un

pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, en un daño irreparable al *hardware* y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina. Casi cualquier medio, una máquina, una cinta, un Route*r, etc,* que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que se generan en los sistemas electrónicos. .

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención; podemos utilizar detectores de agua en los suelos o falsos suelos de las salas de operaciones, y apagar automáticamente los sistemas en caso de que se activen. Medidas de protección menos sofisticadas pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

1.2.1.3 Desastres del entorno

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico, como: picos de tensión, cortes de flujo, sobrecarga de equipos, etc. que a diario amenazan la integridad tanto del *hardware* como de los datos que almacena o que circulan por él.

- **Electricidad**

El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como `picos' porque generalmente duran muy poco: durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al *hardware* o a los datos gracias a que en la mayoría de equipos hay instalados fusibles, elementos que se funden ante una subida de tensión y dejan de conducir la corriente, provocando que la máquina permanezca apagada. Una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo o simplemente hacia cualquier lugar con voltaje nulo.

Un problema que los estabilizadores de tensión o la toma de tierra no pueden solucionar es justamente el contrario a las subidas de tensión: las bajadas, situaciones en las que la corriente desciende por debajo del voltaje necesario para un correcto funcionamiento del sistema, pero sin llegar a ser lo suficientemente bajo para que la máquina se apague.

En estas situaciones la máquina se va a comportar de forma extraña e incorrecta, por ejemplo no aceptando algunas instrucciones, no completando escrituras en disco o memoria, etc.

Otro problema, muchísimo más habitual que los anteriores en redes eléctricas modernas, son los cortes en el fluido eléctrico. Aunque un simple corte de corriente no suele afectar al *hardware*, lo más peligroso son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, las máquinas pueden sufrir daños graves.

La forma más efectiva de proteger lo equipos contra estos problemas de la corriente eléctrica es utilizar una UPS conectada al elemento que queremos proteger. Estos dispositivos mantienen un flujo de corriente estable,

protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen capacidad para seguir alimentando las máquinas incluso en caso de que no reciban electricidad durante cierto periodo de tiempo.

- **Corriente estática**

Es un fenómeno extraño del que la mayoría de gente piensa que no afecta a los equipos, sólo a otras personas. Simplemente tocar con la mano la parte metálica de un conductor puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño, el ordenador sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM.

Contra el problema de la corriente estática existen muchas y muy baratas soluciones: *spray* antiestático, ionizadores antiestáticos...No obstante en la mayoría de situaciones sólo hace falta un poco de sentido común del usuario para evitar accidentes: no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el *hardware*, no mantener el entorno excesivamente seco, etc.

- **Incendios y humo**

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio. .

Un método efectivo contra los incendios son los extintores situados en lugares visibles y de fácil acceso, con capacidad para sofocar diferentes tipos de fuego.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos. Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero hemos de recordar que puede existir humo sin necesidad de que haya un fuego: por ejemplo, en salas de operaciones donde se fuma.

- **Temperaturas extremas**

Las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas.

Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un aire acondicionado. Otra condición básica para el correcto funcionamiento de cualquier equipo es que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU.

1.2.2 Amenazas del Software

Bajo la etiqueta de amenazas existen todo tipo de programas que de una forma u otra pueden dañar los sistemas de computo, éstos fueron creados de forma intencionada (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros).

1.2.2.1 Software incorrecto

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema**,** se denominan *exploits*.

- **Puertas traseras**

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su *software* para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad del sistema.

- **Bombas lógicas**

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas[2]; en ese

[2] Las siguientes secciones de éste capitulo, fueron tomadas principalmente de las direcciones electrónicas: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node72.html a las cuales se les realizó las adecuaciones correspondientes para ser presentadas en la monografía, sin cambiar el contenido temático expuesto en la versión original. De igual manera al ser un documento público y no constar explícitamente los derechos de autor, el autor de la monografía no está incumpliendo las normas estatales en dicho tema.

punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los elementos que la activan comúnmente son: la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado identificador de usuario o la llegada de una fecha concreta.

- **Canales cubiertos**

Los canales cubiertos o canales ocultos, son aquellos que permiten a un proceso transferir información a otros que no están autorizados para leer dicha información.

- **Virus**

Un virus es una secuencia de código que se inserta en un archivo ejecutable (denominado *huésped*), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

- **Gusanos**

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

Un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder al sistema; mientras que una persona, con conocimientos avanzados y medios adecuados que posea, tardaría como mínimo horas en controlar una red completa, un gusano puede hacer eso mismo en pocos minutos.

- **Caballos de Troya**

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario. En la práctica cuando un intruso consigue el privilegio necesario en el sistema instala troyanos para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto.

- **Programas conejo o bacterias**

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.

- **Técnicas salami**

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de dinero de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesos se roban unos centavos, nadie va a darse cuenta de ello.

1.2.3 Amenazas Sobre los Datos

La seguridad física también implica la protección a la información del sistema, tanto a la que está almacenada en él como a la que se transmite entre diferentes equipos.

1.2.3.1 Eavesdropping

La interceptación o *eavesdropping*, también conocida por *passive wiretapping* es un proceso mediante el cual un agente capta información - en claro o cifrada - que no le iba dirigida; esta captación puede realizarse por muchísimos medios. Aunque es en principio un ataque completamente pasivo, lo más peligroso del *eavesdropping* es que es muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo.

Un medio de interceptación bastante habitual es el *sniffing*, consistente en capturar tramas que circulan por la red mediante un programa ejecutándose en una máquina conectada a ella o bien mediante un dispositivo que se engancha directamente el cableado. Estos dispositivos, denominados *sniffers* se conectan en paralelo con el cable de forma que la impedancia total del cable y el aparato es similar a la del cable solo, lo que hace difícil su detección. Contra estos ataques existen diversas soluciones; la más barata a nivel físico es no permitir la existencia de segmentos de red de fácil acceso, lugares idóneos para que un atacante conecte uno de estos aparatos y capture todo nuestro tráfico. Tampoco debemos descuidar las tomas de red libres, donde un intruso con un portátil puede conectarse para capturar tráfico; es recomendable analizar regularmente nuestra red para verificar que todas las máquinas activas están autorizadas.

1.2.3.2 Backups

Un error muy habitual es almacenar los dispositivos de *backup* en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto,

que en principio puede parecer correcto y cómodo si necesitamos restaurar unos archivos, puede convertirse en un problema: si se produce un incendio de grandes dimensiones. Como podemos ver, resulta recomendable guardar las copias de seguridad en una zona alejada de la sala de operaciones, aunque en este caso descentralicemos la seguridad y tengamos que proteger el lugar donde almacenamos los *backups* igual que protegemos la propia sala o los equipos situados en ella.

También suele ser común etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido (sistemas de ficheros almacenados, día y hora de la realización, sistema al que corresponde, etc.); esto tiene una parte positiva y una negativa. Por un lado, recuperar un fichero es rápido: sólo tenemos que ir leyendo las etiquetas hasta encontrar la cinta adecuada. Sin embargo, igual que para un administrador es fácil encontrar el *backup* deseado también lo es para un intruso que consiga acceso a las cintas, no necesita vulnerar el cortafuegos, conseguir una clave del sistema o chantajear a un operador: nosotros mismos le estamos poniendo en bandeja toda nuestros datos.

Como medida de protección se puede diseñar cierta codificación que sólo conozcan las personas responsables de las copias de seguridad, de forma que cada cinta vaya convenientemente etiquetada, pero sin conocer el código sea difícil imaginar su contenido. Y si aún pensamos que alguien puede sustraer todas las copias, simplemente tenemos que realizar *backups* cifrados...y controlar más el acceso al lugar donde las guardamos.

1.2.3.3 Otros elementos

En muchas ocasiones los responsables de seguridad de los sistemas tienen muy presente que la información a proteger se encuentra en los equipos, en

las copias de seguridad o circulando por la red (y por lo tanto toman medidas para salvaguardar estos medios), pero olvidan que esa información también puede encontrarse en lugares menos obvios, como listados de impresora, facturas telefónicas o la propia documentación de una máquina.

Como medida de protección, las impresoras, *plotters*, faxes, o cualquier dispositivo por el que pueda salir información del sistema ha de estar situado en un lugar de acceso restringido.

Otros elementos que también pueden ser aprovechados por un atacante para comprometer la seguridad del sistema son los manuales de sistemas operativos utilizados, facturas de teléfono pueden indicar los números del módems o agendas de operadores que revelan los teléfonos de varios usuarios para hacer ingeniería social con ellos. Aunque es conveniente no destruir ni dejar a la vista de todo el mundo esta información, si queremos eliminarla, es recomendable utilizar una trituradora de papel, dispositivo que dificulta muchísimo la reconstrucción y lectura de un documento destruido.

1.2.4 Herramientas de Seguridad.

Cualquier herramienta de seguridad representa un arma de doble filo, de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host* o de una red completa.

1.3 ADMINISTRADORES, USUARIOS Y PERSONAL

El punto más débil de cualquier sistema informático son las personas relacionadas en mayor o menor medida con él; desde un administrador sin una preparación adecuada o sin la suficiente experiencia, hasta un guardia de seguridad que ni siquiera tiene acceso lógico al sistema, pero que deja acceder a todo el mundo a la sala de operaciones, pasando por supuesto por la gran mayoría de usuarios, que no suelen ser conscientes que la seguridad también les concierne a ellos. Frente a cada uno de estos grupos (administradores, usuarios y personal externo al sistema) un potencial atacante va a comportarse de una forma determinada para conseguir lograr sus objetivos, y sobre cada uno de ellos ha de aplicarse una política de seguridad diferente. .

Hasta ahora se ha hablado de posibles ataques relacionados con el personal de un sistema informático; sin embargo, existen otras amenazas a la seguridad provenientes de ese personal que no son necesariamente intencionados, se podrían catalogar como accidentes, pero el que la amenaza no sea intencionada no implica que no se deba evitar: decir '*no lo hice a propósito'* no va ayudar para nada a recuperar unos datos perdidos.

A continuación se presenta una relación de los elementos que pueden amenazar el sistema:

1.3.1 Personal

Aunque los ataques pueden ser intencionados, en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas...y sus debilidades, lo normal es que más que ataques se trate de *accidentes* causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de

mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros; y en el primer caso, el ‘atacante' ni siquiera ha de tener acceso lógico ni físico a los equipos, ni conocer nada sobre seguridad en Sistemas Operativos.

1.3.2 Ex-empleados

Otro gran grupo de personas potencialmente interesadas en atacar el sistema, son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia. Generalmente, se trata de personas descontentas con la empresa, que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo: amparados en excusas como ‘*No me han pagado lo que me deben'*, pueden insertar troyanos, bombas lógicas, virus...o simplemente conectarse al sistema como si aún trabajaran para la organización.

1.3.3 Curiosos

Junto con los *crackers*, los curiosos son los atacantes más habituales de sistemas; y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto.

1.3.4 Crackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un

simple *exploit* los equipos que presentan vulnerabilidades; esto convierte a las empresas en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos y a veces más peligrosos, hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otras empresas.

1.3.5 Terroristas

Bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

1.3.6 Intrusos Remunerados

Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte, generalmente para robar secretos o simplemente para dañar la imagen de la entidad afectada.

1.4 ¿COMO NOS PODEMOS PROTEGER?

Para proteger el sistema se debe realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis se debe diseñar una política de seguridad que defina responsabilidades y reglas a seguir para minimizar sus efectos en caso de que se produzcan.

Los mecanismos de protección se dividen en tres grandes grupos: de prevención, de detección y de recuperación.

1.4.1 Mecanismos de Prevención

Son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones en la red.

1.4.2 Mecanismos de Detección

Se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoria como *Tripwire*.

1.4.3 Mecanismos de Recuperación

Son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el *hardware* adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado:

1.4.3.1 Mecanismos de análisis forense

Su objetivo es averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

2. POLÍTICA DE SEGURIDAD INFORMÁTICA

Todos los miembros de una empresa u organización deben tener sentido de pertenencia y estar comprometidos con la protección de sus recursos. Esta preocupación, no debe ser solamente de los directivos de la empresa, puesto que el éxito de toda política de seguridad, radica en el compromiso que tenga todo el personal en proteger sus activos.

DEFINICIÓN DE POLÍTICA DE SEGURIDAD

La política de seguridad informática es un compendio de normas, procedimientos e instrucciones que describen la forma adecuada para usar los recursos de un sistema de computo, las responsabilidades y el qué hacer ante la presencia de un incidente de seguridad; así como también la estandarización del método de operación de cada uno de los responsables de la seguridad de la información.

Con un eficiente esquema de políticas de seguridad, los administradores mitigan los riesgos y les permiten actuar de manera rápida y acertada ante la presencia de una amenaza computacional. Para los usuarios, les sirve de guía en el manejo adecuado del sistema, lo que se puede o se debe hacer para minimizar los riesgos de un posible incidente de seguridad informático.

ELABORACION DE LA POLÍTICA DE SEGURIDAD

Para definir en forma adecuada y eficiente una política de seguridad se deben tener en cuenta varios aspectos como:

Aspecto Tecnológico

En el aspecto tecnológico se debe tener en cuenta el apoyo económico y la inversión que realicen las empresas en la adquisición del hardware necesario para mejorar la seguridad de la información (Servidores, Firewalls, Routers, Switches, Cámaras, etc.), adecuación de la planta física (áreas de acceso restringido, pisos y techos adecuados, extintores adecuados para los diferentes tipos de conflagraciones y ubicados estratégicamente, etc.), la adquisición y actualización del software (sistema operativo, software de aplicación, utilidades, programas de diagnostico, etc.) y la correcta administración de los datos (copias de seguridad, registros de auditoria, bases de datos, etc.).

También es muy importante realizar un listado con todos los elementos con los que cuenta la empresa, como el hardware, software y los datos, que necesitan protección, con el objetivo de identificar las vulnerabilidades existentes.

Aspecto Humano

El aspecto humano es fundamental en el cumplimiento de los objetivos propuestos por las empresas, con la implantación de una política de

seguridad; puesto que de nada sirve realizar una inversión significativa en la adquisición de hardware de última tecnología y software actualizado en la detección amenazas a la seguridad; si el personal administrativo, operativo o comercial, no es consciente de su importancia y compromiso en la disminución del riesgo en cada una de sus áreas de trabajo.

Comité de Seguridad

Se debe conformar un equipo multidisciplinario, el cuál se debe reunir periódicamente, de acuerdo a un cronograma de actividades, para analizar, discutir, reglamentar y elaborar un documento con la política de seguridad de la empresa.

Documento Final

En la elaboración del documento final se debe utilizar un lenguaje poco técnico, fácil de entender y que sea accesible a todo el personal; la información debe ser clara, concisa y ajustarse a la realidad de la empresa.

Etapas de Producción

Para diseñar e implementar la política de seguridad de la información en cualquier empresa, se debe tener un conocimiento claro de la estructura organizacional, de la misión y visión de la misma y de los procesos que se desarrollan, con el objetivo de identificar las vulnerabilidades, las cuales se convierten en los puntos primordiales de analizar. El trabajo de producción se compone de las siguientes etapas:

- Objetivos y ámbito.
- Entrevistas
- Investigación y análisis de documentos.
- Reunión de política
- Glosario
- Responsabilidades y penalidades.

Hacer Oficial la Política de Seguridad Informática

El documento final será revisado y aprobado por el área administrativa de la empresa y debe ser publicado y comunicado en forma adecuada a todos los empleados, socios, clientes, etc.

DOCUMENTOS DE LA POLÍTICA DE SEGURIDAD

El comité de seguridad debe realizar reuniones y entrevistas con todo el personal de la empresa, con el objetivo de identificar los riesgos existentes, los procesos que ejecutan y la preocupación que existe en los empleados en proteger los activos de la empresa. Estas reuniones permiten generar un listado con todas las vulnerabilidades encontradas; a las cuales se debe realizar una valoración del nivel de riesgo, cuantificar el costo asociado y las medidas de contención que se deben implementar, para minimizar el riesgo existente.

Producto de la información recolectada y analizada por el comité de seguridad, se debe elaborar un documento final, el cuál debe contener:

- La descripción clara de los elementos involucrados en la política de seguridad.

- La declaración del área administrativa, que apoye la legislación y cláusulas contractuales, la capacitación y formación en seguridad de la información y los mecanismos de prevención contra amenazas (virus, hackers, accesos físicos no autorizados, etc.)
- Responsabilidades de cada uno de los usuarios y personal involucrado; donde quede claro las funciones realizadas y su nivel de compromiso con la seguridad de la empresa.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas.
- Definición de las violaciones a la seguridad y las sanciones que puede recibir cualquier empleado, socio o cliente que no cumpla con la política de seguridad de la información.

También debe contener con un glosario de terminología amplio, con el objetivo de despejar cualquier duda existente.

MODELO DE ESTRUCTURA DE LA POLITICA DE SEGURIDAD

El documento que recopila la política de seguridad debe estar basado en un estándar, como el planteado a continuación, que tiene tres secciones principales:

- **Directrices:** Son reglas generales de nivel estratégico que se fundamentan en la misión y visión de la empresa. Recopilan todos los valores que se deben seguir para garantizar que la información tenga el nivel de seguridad exigido.
- **Normas:** Son reglas generales y especificas de nivel táctico, que pueden ser especificas para el publico que se destinan, por ejemplo *para técnicos*

puede ser el periodo de cambio de claves, copias de seguridad, acceso físico, etc. o *normas para usuarios* que son basadas en aspectos más genéricos como cuidado de claves, cuidado de equipos, etc.

- **Procedimientos e instrucciones de trabajo:** son orientaciones para realizar una actividad operativa de seguridad o comandos a ser ejecutados en el momento de realizar un procedimiento; un modelo paso a paso para los usuarios.

ACOMPAÑAMIENTO DE LA POLITICA

Para que la política de seguridad sea efectiva, necesita contar con tres elementos:

Cultura

El área administrativa es fundamental en el cambio cultural que deben experimentar sus empleados, tanto en la implementación de capacitaciones periódicas, que minimicen el nivel de riesgo, como en la asignación de funciones, privilegios o responsabilidades de acuerdo a las actividades que tiene cada usuario.

Herramientas

Se debe contar con un recurso humano capacitado y eficiente en la ejecución de procesos, un recurso económico suficiente para la adecuación de planta física y para la adquisición de hardware y software requerido, y herramientas de automatización y control acordes con las necesidades de la empresa.

Monitoreo

La política de seguridad debe ser monitoreada constantemente, con la posibilidad de realizarle ajustes, de acuerdo a las nuevas amenazas encontradas o a los cambios tecnológicos o administrativos presentados.

IMPLANTACIÓN DE LA POLITICA DE SEGURIDAD

Para realizar la implantación de la política de seguridad se deben cumplir ciertos requisitos como:

- Realizar una adecuada divulgación, que involucre personal administrativo, socios, empleados, usuarios, clientes, etc.
- La política de seguridad debe estar disponible, para ser consultada en cualquier momento. Puede estar publicada en la Intranet de la empresa, o enviada al correo electrónico de todos los interesados.
- Se deben programar capacitaciones, charlas de divulgación, entrenamientos continuos a todo el personal; en especial a los ingresados recientemente.

USOS DE LA POLÍTICA DE SEGURIDAD

Después de realizarse la planificación, el análisis, desarrollo e implementación de la política de seguridad en la empresa, ésta permite:

- Definir diferentes tipos de controles sobre los procesos desarrollados en cada una de las áreas de la empresa.
- Establece los accesos permitidos a los usuarios dependiendo de sus funciones.

- Orienta a los usuarios en los procedimientos que deben evitar para disminuir las vulnerabilidades de la empresa.
- Establece los procedimientos a seguir, si se sospecha de un posible ataque o violación a la seguridad.
- Permite escoger la mejor tecnología en la adquisición de hardware y software.
- Establece las responsabilidades e implicaciones que tiene un usuario, al permitir una violación de seguridad o realizar un delito informático.

Después de implantada la política de seguridad se deben realizar varios controles que garanticen su adecuado funcionamiento y realizar actualizaciones periódicas en normas, procedimientos, funciones, sanciones, etc.

3. DISEÑO DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA CELTEL S.A.

A continuación se muestra el desarrollo de la Política de Seguridad Informática, para la empresa "Celulares y Telecomunicaciones CELTEL S.A.", siguiendo los aspectos definidos en capítulos anteriores.

ASPECTO TECNOLÓGICO

En el aspecto tecnológico la empresa CELTEL S.A. cuenta con los siguientes recursos:

Hardware.

- **Routers y Switches**

La empresa CELTEL S.A. tiene en la oficina principal, área administrativa de San Gil (Santander) tres routers Dlink (dos en actividad y uno de respaldo) y cuatro switches marca 3Com (dos en actividad y dos de respaldo). Cada una de las 20 oficinas sucursales de la empresa, cuenta con un Router Dlink y uno Switch 3Com.

Figura 2 Routers y Switches CELTEL S.A.

Tabla 1 Características de los Routers.

Cantidad	Marca	Características
3	D'LINK	Estandares: IEEE 802.3 10BaseT ETHERNET / IEEE 802.3u 100BaseTX FAST. Funciones Internet Server: NAT DHCP Server VPN: PPTP, L2TP e IPSec. Modalidad pass-through. Funciones de Firewall: MAC Filtering/ IP Filtering/URL Filtering/ Domain Blocking/ Scheduling

Tabla 2 Características de los Switches.

Cantidad	Marca	Características
2	3COM	8 PUERTOS 10/100BASE-TX/RJ-45 Store-and-forward, full-half-duplex auto-negotiation Input: 230V 50Hz 0.1A Output: 12V 1000mA
2	3COM	16 PUERTOS 10/100 Ethernet con detección automática, Interface 10/100BASE-TX/RJ-45 Store-and-forward, full-half-duplex auto-negotiation Input: 230V 50Hz 0.1A Output: 12V 1000mA

- **Servidores**

La empresa CELTEL S.A. cuenta con dos servidores de bases de datos, en los cuales están implementadas las aplicaciones necesarias para el desarrollo de sus actividades comerciales; un servidor Proxy que actúa como intermediario entre el programa cliente (Internet Explorer) y el servidor de base de datos a acceder y un Firewall que actúa como dispositivo de seguridad; éstos se encuentran ubicados en el cuarto de equipos, tercer piso del edificio administrativo en San Gil (Santander).

Figura 3 Servidores de Datos, Proxy y Firewall de la Empresa CELTEL S.A.

Tabla 3 Características de los servidores.

Cantidad	Marca	Características
1	DELL PowerEdge 1800	Dos procesadores Intel® Xeon™ con tecnología de 64 bits de memoria ampliada[1] hasta 3,4 GHz; **Bus frontal** 800 MHz; **Chipset** Intel E7250; **Memoria** 4,1GB / 12 GB DDR2 400 SDRAM; 4 **Unidades de disco duro de** 80 GB(7.200 rpm) SATA; **Vídeo** ATI Radeon 7000-M incorporado con SDRAM de 16 MB
1	DELL PowerEdge SC423	Dos procesadores Intel® a de 64 bits; **Bus frontal 6**00 MHz; **Memoria** 2 GB DDR2 400 SDRAM; 4 **Unidades de disco duro de** 80 GB(7.200 rpm).
2	DELL Precision 270	Un procesador Intel®; Pentium IV (un solo núcleo) Tecnología Hiper Threading; Cache de 2 MB; **Chipset** Intel 975 de 64 bits; 4 Gb **Memoria SDRAM** DDR2 a 533 MHz; 4 **Unidades de disco duro de** 80 GB(7.200 rpm) SATA.

- **Equipos de cómputo**

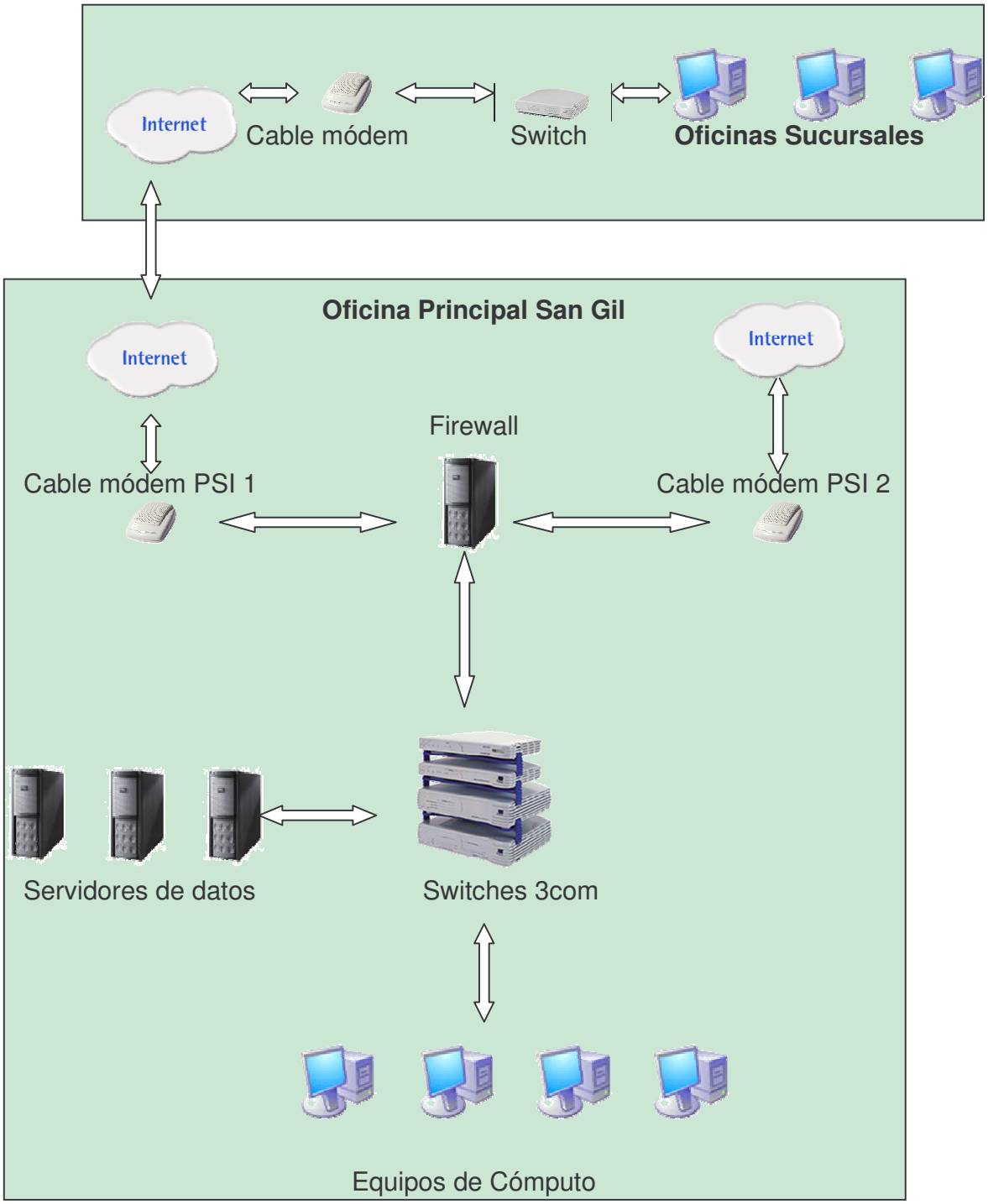
La empresa CELTEL S.A. tiene en la oficina principal, área administrativa de San Gil (Santander) once estaciones de trabajo y cuatro equipos portátiles; cuyas características se describen a continuación en la siguiente tabla.

Tabla 4 Características de los equipos de cómputo.

Cantidad	Marca	Características
5	HP COMPAQ	Procesador Celeron de 2,54 GHz, Memoria Ram de 512 MB, Disco Duro de 80 GB, Monitor LCD de 14', Teclado y mouse.
6	DELL	Procesador Celeron de 2,54 GHz, Memoria Ram de 512 MB, Disco Duro de 80 GB, Monitor LCD de 14', Teclado y mouse.
4	PORTATIL DELL LATITUDE D510	Procesador Intel Centrino de 1,8 GHz, Memoria Ram de 512 MB, Disco Duro de 60 GB.

En la actualidad hay 20 sucursales en todo el país, las cuales cuentan con cinco o seis estaciones de trabajo aproximadamente por sucursal; cuyas características son similares a las existentes en la oficina principal.

Figura 4 Diagrama de Red de Datos de la Empresa CELTEL S.A.



3.1.2 Software

- **Sistema operativo**

Los Servidores tienen como plataforma el sistema operativo LINUX FEDORA CORE 4.

Las estaciones de trabajo utilizan como plataforma el sistema operativo WINDOWS XP PROF Versión 2002 Service Pack 2.

- **Software de aplicación**

La empresa CELTEL S.A. es uno de los distribuidores de telefonía móvil celular de COMCEL en Colombia; tiene implementada una aplicación propia, para el control de inventario denominada ‘’ATLAS’’, y otra aplicación llamada “ZEUS” para el registro contable y liquidación de la nomina de sus empleados.

3.1.3 Datos

En el servidor de base de datos de CELTEL S.A. se encuentra una aplicación que maneja el inventario y comercialización de telefonía celular, simcard y accesorios en planes prepago y pospago; de igual forma se lleva un registro de los subdistribuidores, asesores y clientes de las diferentes bodegas y oficinas que tiene la empresa a nivel nacional. En el servidor ZEUS se maneja la parte administrativa, contable y financiera de la empresa.

3.1.4 Aspecto humano

En el aspecto humano la empresa CELTEL S.A. agrupa más de 100 (cien) empleados a nivel nacional, organizados jerárquicamente en una estructura administrativa, operativa y comercial. La sección administrativa esta conformada por la junta de socios, la gerencia general, 10 (diez) profesionales de diferentes áreas que laboran en la ciudad de Sangil (Santander) y 3 (tres) gerencias regionales en las ciudades de Bogotá, Bucaramanga y Medellín. La sección operativa esta conformada por un gerente comercial en cada departamento y 1 (un) coordinador o administrador en cada oficina sucursal y la sección comercial esta integrada por el grupo de asesores comerciales que laboran en cada una de las 25 oficinas distribuidas en los departamentos de Cundinamarca, Antioquia y Santander.

3.2 COMITÉ DE SEGURIDAD

El comité de seguridad esta integrado por las siguientes personas:

Andrés Rivero: Delegado de la junta de socios.
Tatiana Ferreira: Gerente general.
Henry Javier Barón: Ingeniero de sistemas, director del proyecto “Atlas”
Luis Eduardo García: Ingeniero de sistemas, Soporte técnico.
Rubiela Serrano: Contadora.
Claudia Prada: Auditora.
Carmen Elisa Espítia: Abogada.

3.3 ETAPAS DE PRODUCCIÓN

3.3.1 Entrevistas

El comité de seguridad programó una serie de entrevistas a todo el personal que integra cada una de las diferentes áreas de trabajo (Sistemas, Contabilidad, Inventarios, Penalizaciones, Comercial, Auxiliar Administrativo, Servicios Generales, etc) con el objetivo de identificar las vulnerabilidades en seguridad existentes y el compromiso que tiene cada uno de ellos en proteger los activos de la empresa.

3.3.2 Evaluación del riesgo

La evaluación del riesgo es el proceso de identificar, cuantificar y minimizar las amenazas que pueden afectar los recursos de un sistema. Una amenaza como ya se mencionó en capítulos anteriores es cualquier fuerza o fenómeno que pueda degradar la disponibilidad, integridad o confidencialidad de un recurso del sistema de información. El secreto para el manejo efectivo del riesgo es la capacidad para calificar, cuantificar y reducirlo a niveles aceptables.

El servidor Atlas es un equipo que se encuentra instalado y configurado en la sede principal de la empresa CELTEL S.A., el cuál es accesado diariamente por las diferentes bodegas y oficinas a nivel nacional para complementar sus procesos de inventario y comercialización de equipos celulares en prepago y pospago. Cuenta con varios módulos como el de creación de usuarios y productos, manejo y control de inventarios, administración de periodos, facturación, entre otros.

El servidor Zeus es un equipo que se encuentra instalado y configurado en la red LAN de la sede principal de la empresa CELTEL S.A., el cual es una herramienta importante en el desempeño de las labores administrativas, contables y financieras de la empresa. Cuenta con varios módulos como el

de mantenimiento y consulta de hoja de vida de los empleados de cada una de las sucursales, liquidación mensual de nomina y liquidación periódica de primas y cesantías, entre otros.

3.3.2.1 Amenazas en los servidores y equipos de cómputo de CELTEL S.A. y medidas de contención.

Tabla 5 Amenazas a los Servidores y Equipos de Cómputo de CELTEL S.A.

Amenaza
Fluctuaciones en la tensión o frecuencia en el suministro de energía eléctrica, tales como: corte total de energía, baja tensión, variaciones en la frecuencia, picos de alta tensión, sobre tensión y caídas de tensión.
Nivel de Riesgo: Alto
Costo Asociado
Las variaciones y cortes en el fluido eléctrico pueden afectar los equipos en sus diferentes componentes de hardware, como fuente de poder, tarjetas de circuitos, memoria y principalmente en la lectura y grabación en discos duros, siendo la perdida de la información la peor consecuencia. Aunque los costos por daño en el hardware son fácilmente calculables, no lo es igual para determinar la indisponibilidad de los servidores en cualquier momento que se requiera. Esto generaría traumatismos en la realización de procesos en los diferentes puntos de venta a nivel nacional, ventas represadas o perdida de ventas de los productos que se comercializan, entre otros.
Medidas de Contención

El suministro de energía posee inevitables variaciones de tensión (220 v) así como de frecuencia (50 hz) y de la forma de onda (senoidal), afectando el funcionamiento de los aparatos electrónicos. En el área administrativa de la empresa CELTEL S.A. se adquirieron 7 UPS marca Power Back 600 VA para las principales estaciones de trabajo y una UPS para los servidores de datos, marca APC-Smart-UPS 3000 con las siguientes características:

Salida

Capacidad de Potencia de Salida:	2250 Vatios / 3000 VA.
Máxima Potencia Configurable:	2250 Vatios / 3000 VA.
Tensión de Salida nominal:	230 V
Distorsión de tensión de salida:	menos del 5% con carga completa.

Entrada

Entrada de voltaje:	230 V.
Frecuencia de entrada:	50/60 Hz +/- 3 Hz (Autosencible)
Longitud del cable:	2 Mts.
Tipo de batería:	Batería sellada de plomo sin necesidad de mantención con electrolito suspendido a prueba de filtración.

Amenaza

Daño o deterioro de algunos de los componentes Hardware de los equipos (tarjetas, placas base, memorias, discos duros, fuente de poder, tarjetas de circuitos, etc.)

Nivel de Riesgo: Medio

Costo Asociado

En caso de daño de algún componente Hardware, los servidores no van a estar disponibles durante el tiempo que se tarde en repararlo, generando demoras en la realización de diferentes procesos a nivel nacional y el costo asociado es directamente proporcional al periodo de inactividad del equipo. En caso de daño de alguno de los discos duros, el principal problema es la recuperación de la información, mientras que en los demás componentes hardware el periodo

de inactividad depende del tiempo que lleve remplazar la pieza dañada.
Medidas de Contención
Existen varias medidas de contingencia para minimizar el tiempo de inactividad que puede permanecer un equipo. Algunas de ellas son: 1. Se tiene a disposición un disco de cambio rápido (hot swap), que permite ser removidos en caliente, es decir cuando aún se encuentra encendido el equipo, sin necesidad de interrumpir la conexión con el sistema operativo. Lo cual hace posible que si algún elemento de hardware llega a fallar, se pueda retirar el disco e insertarlo en otro equipo con la misma configuración que el primero. 2. Se realizan copias de seguridad diarias en los servidores y semanales, quincenales o mensuales en las estaciones de trabajo, dependiendo del grado de importancia de la información manejada; para minimizar el periodo de inactividad de los equipos en caso de presentarse algún daño físico. Se realizan periódicamente mantenimientos preventivos a los servidores y estaciones de trabajo, para minimizar los riesgos por daño de hardware en los equipos de cómputo.
Amenaza
Elevada temperatura en el cuarto de equipos
Nivel de Riesgo: Alto
Costo Asociado
El incremento en la temperatura puede ocasionar daños en el hardware de los servidores o deficiencia en el rendimiento de los mismos; provocando indisponibilidad del servicio.
Medidas de Contención

La temperatura adecuada es fundamental para el óptimo rendimiento de los equipos de cómputo; por esto, fue necesario instalar un sistema de aire acondicionado para regular la temperatura en el cuarto de equipos.
Amenaza
Incendio
Nivel de Riesgo: Medio
Costo Asociado
Las instalaciones eléctricas defectuosas son una potencial fuente de de incendios. Un incendio conduce a la pérdida total o parcial de las instalaciones físicas, de los equipos y de la información en caso de no tener copias de respaldo almacenadas en otras localidades o dependencias.
Medidas de contención
Se deben tener en cuenta las siguientes recomendaciones, para prevenir o minimizar los efectos causados por un incendio: ▪ Paredes de material incombustible. ▪ Techos resistentes al fuego. ▪ Canaletas y aislantes resistentes al fuego. ▪ Detectores de fuego alejados del aire acondicionado. ▪ Alarmas de incendio. ▪ Evitar sobrecargar la red eléctrica, por conexiones de múltiples equipos a la misma toma o punto eléctrico, o también sobre saturar la capacidad de la red eléctrica que inicialmente fue diseñada**.** ▪ Ubicar estratégicamente en las áreas de trabajo, los diferentes tipos de extintores para ser utilizados en caso de presentarse un incendio, de acuerdo al origen del fuego: H2O, CO2, Espuma, Polvo seco, etc. ▪ Evitar realizar conexiones o reparaciones eléctricas, cuando no exista personal capacitado para ésta función.
Amenaza

Acceso Físico
Nivel de Riesgo: Alto
Costo Asociado
La falta de controles en el acceso físico del personal al cuarto de equipos, hace inútiles todas las medidas de seguridad que se hayan implementado en la red. Se puede producir accidentes, robo o extravío de elementos físicos o de información (listados, copias de seguridad, etc.), que puede ser destruida, modificada o simplemente leída para ser utilizada en forma inapropiada o malintencionada.
Medidas de Contención
Es importante crear o identificar zonas de acceso restringido y poner en práctica las normas de seguridad que ayuden a minimizar los riesgos que puedan presentarse. En el caso de CELTEL S.A. se cambiaron las guardas (chapas) del cuarto de equipos y oficina contigua; se restringió el acceso de personal no autorizado, así como el acceso de comidas y bebidas al cuarto de equipos o áreas de trabajo. Se recordó al personal la importancia de cumplir las normas de seguridad correspondientes a cada área de trabajo.
Amenaza
Puntos de red expuestos.
Nivel de Riesgo: Alto
Costo Asociado
Al no ejercer un estricto control sobre los puntos de red que están siendo utilizados, se abren las posibilidades para que un atacante pueda acceder a la información, para modificarla, destruirla, infectarla con virus o leerla con propósitos malintencionados.

Medidas de Contención
Se bloquearon los puntos de red que no están siendo utilizados; especialmente los ubicados en lugares apartados. Se realizan análisis de tráfico frecuentes.
Amenaza
Sistema de archivos o ficheros en Linux
Nivel de Riesgo: Alto
Costo Asociado
La asignación de permisos en Linux, determina cuales archivos pueden ser leídos, modificados o ejecutados. Un error en la asignación de permisos puede generar graves problemas de seguridad en la información. La correcta asignación de los permisos, atributos y controles es vital para la seguridad del sistema.
Medidas de Contención
Existen en Linux tres tipos básicos de archivos: Archivos planos, directorios y ficheros especiales (dispositivos). Los permisos de cada fichero son la protección básica de estos objetos en el sistema operativo. El esquema de protección, consiste en dividir los usuarios en tres grupos: ▪ La clase *u* (user), formado únicamente por el dueño del fichero. ▪ La clase *g* (group), formada por todos los usuarios que pertenecen al mismo grupo. ▪ La clase *o* formada por el resto de usuarios. Un usuario puede pertenecer a más de un grupo, pero un archivo solo puede pertenecer a un grupo. Existen tres formas de acceder a un archivo: lectura, escritura y ejecución. Así los nueve bits de protección de acceso de cada archivo se encuentran divididos en tres grupos de tres bits. Cada grupo de tres bits indica el acceso a *u, g, o*, respectivamente, y cada bit de cada grupo indica: Bit 1 (*r* **),** permiso de lectura.

Bit 2 (*w* **),** permiso de escritura.
Bit 3 (*x* **),** permiso de ejecución.

El usuario *root* decide, qué usuarios pertenecen a qué grupos y cuales se suelen organizar de acuerdo a sus razones de trabajo.
Contra éstos ataques, se deben comparar frecuentemente los permisos asignados a los archivos o listados más importantes y sí se encuentra que alguno tiene una lista de control que otorga permisos no reflejados en los bits *r w x,* se debe analizar dicha lista y verificar que todo este correcto. Es recomendable programar shellscrips, que automaticen éstos procesos e informen en el caso que algo sospechoso se detecte.

Amenaza

Modificación mal intencionada del software de aplicación.

Nivel de Riesgo: Alto

Costo Asociado

La modificación del software de aplicación y del propio núcleo del sistema operativo, por bugs generados en el desarrollo del mismo, se constituye en una de las mayores amenazas a la seguridad de cualquier sistema informático. Uno de los errores más utilizados por atacantes es el stack smashing o desbordamiento de pila, también conocido como *buffer overflow*. Otra amenaza que se encuentra disponible en Internet son los *exploits* (programas que aprovechan los errores de otros programas, para violar la política de seguridad del sistema o ganar privilegios sobre éste).

Éste tipo de ataques pueden ocasionar la inutilización total o parcial de los equipos, con costos elevados, si no se tienen las herramientas necesarias y los backups o equipos de respaldo para minimizar los efectos causados.

Medidas de Contención

Se debe analizar regularmente el tráfico de la red. El administrador del sistema debe instalar software proveniente de fuentes confiables y tomar las precauciones necesarias para ejecutar planes de contingencia ante posibles ataques o daños en los equipos. Otra medida de contención es la actualización periódica de las aplicaciones instaladas en los sistemas, de acuerdo a las nuevas versiones que se van liberando con las correcciones de problemas de seguridad y errores detectados en las anteriores versiones.
Amenaza
Divulgación, interceptación o perdida parcial o total de los datos.
Nivel de Riesgo: Alto
Costo Asociado
La interceptación o *eavesdropping,* es un proceso pasivo, mediante el cual un agente capta información (cifrada o no) que no le iba dirigida. El problema del *eavesdropping* es que es muy difícil de detectar mientras se produce, de forma que el atacante puede capturar información privilegiada y claves para acceder a más información, sin que nadie se de cuenta, hasta que dicho atacante utiliza la información capturada; convirtiendo el ataque en activo.
Medidas de Contención
La seguridad a los datos implica tanto la protección de la información almacenada, como la que se transmite entre los diferentes equipos. Contra los ataques de interceptación existen diversas soluciones; como la utilización de software de cifrado o encriptación para realizar comunicaciones o almacenar información. A nivel físico, se deben administrar y supervisar las tomas de red libres, para evitar que un intruso se conecte y capture el tráfico de la red. Existen soluciones más costosas y efectivas contra la interceptación, como la utilización de cableado en vacío para evitar la interceptación de datos que

viajan por la red.

Las copias de seguridad son los medios más utilizados por los administradores para restaurar un sistema que ha dejado de funcionar correctamente, por diferentes motivos. Por está razón es necesario seguir las siguientes recomendaciones para garantizar la seguridad de la información:

- Verificar el correcto funcionamiento de la copia de seguridad, después de haberse realizado.
- Etiquetar las copias de seguridad con un código, que sea comprensible para el administrador, pero que no suceda lo mismo con el atacante que roba el medio de almacenamiento. Proporcionar en la etiqueta información detallada del contenido de la copia de seguridad, no es adecuado, porque se permite el acceso a la información en una forma fácil.

La ubicación de las copias de seguridad es un aspecto importante. No es adecuado almacenarlas en el mismo sitio de los sistemas (cuarto de equipos o el mismo edificio), ante la posibilidad de presentarse un desastre del entorno, como un incendio o inundación. Una buena política de seguridad de los backups es tener un juego de copias en otro edificio con las políticas de seguridad adecuadas y otro juego de copias en el cuarto sistemas, donde se le facilite al administrador la recuperación de la información en cualquier momento.

Amenaza
Manejo de contraseñas.
Nivel de Riesgo: Alto
Costo Asociado

El uso inadecuado de contraseñas, hace más vulnerable la seguridad de cualquier sistema informático.

En el sistema operativo Linux la clave o password, se almacenan generalmente en el fichero /etc/passwd. Donde se almacena la información de cada usuario

en una línea de texto, separando los diferentes campos con el carácter "**:**" de la siguiente manera: En primer lugar aparece el login del usuario y la clave cifrada; a continuación el identificador del usuario y el grupo respectivamente, el siguiente campo corresponde a la información administrativa con la identidad real del usuario, los dos últimos campos corresponden al directorio del usuario y al shell que le ha sido asignado.

Ejemplo:

Publico:x:1300:100:PUBLICO:/disco2/biblio:/bin/sh

En el sistema operativo Linux lo que distingue un usuario de otro es el UID, el login es utilizado para comodidad de las personas. Si en /etc/passwd existen dos entradas con un mismo UID, para el sistema operativo Linux, se trata del mismo usuario, aunque tengan un login y un password diferente. Esto es aprovechado por los atacantes que han conseguido privilegios de administrador en una maquina; añadiendo una línea /etc/passwd mezclada entre las demás con nombre de usuario normal pero con UID en 0; así garantizan la entrada al sistema como administradores.

Los ataques de texto cifrado escogido constituyen la principal amenaza al sistema de autenticación de Linux; no es fácil descifrar contraseñas, pero es muy fácil cifrar una palabra y comparar el resultado con la cadena almacenada en el fichero de claves, /etc/passwd. De ésta forma el atacante leerá el fichero de claves y mediante un software como Crack, cifrará todas las palabras de un fichero denominado diccionario comparando el resultado obtenido con la clave cifrada del fichero de contraseñas; si ambos coinciden, ya ha obtenido una clave para acceder al sistema de forma no autorizada.

Medidas de Contención

Se han diseñado diferentes medidas de contención para minimizar las debilidades presentes en el sistema de autenticación de Linux. La principal forma de evitar ataques de texto cifrado escogido es utilizar passwords que no utilicen palabras de los diccionarios típicos: nombres propios, utilizando

combinaciones débiles como javier0256, nombres de lugares, actores, personajes, etc. Para ello existen herramientas como *Npasswd y Passwd+* para crear contraseñas fuertes que utilizan combinaciones de minúsculas y mayúsculas, números mezclados con texto, símbolos como &, $, %, o #, etc. Es recomendable que el administrador del sistema ejecute con cierta periodicidad programas adivinadores, tipo crack, para comprobar que sus usuarios no hayan elegido contraseñas débiles, e insistir a los usuarios que mantengan sus contraseñas en secreto.

Una opción que se utiliza regularmente es la utilización de software orientado a la generación automática de contraseñas no crackeables como *Password Depot,* el cuál utiliza algoritmos de encripción robustos como BlowFish y Rijndael, permite salvar todos los passwords de las diferentes cuentas en una sola lista, lo cual permite que el usuario no necesite memorizar sus passwords, porque la herramienta posee la utilidad de insertar las claves en donde se necesite, arrastrándolas y soltándolas con el mouse.

Existen otros métodos para proteger las contraseñas de los usuarios como el Oscurecimiento de contraseñas (Shadow Password), el cual consiste en impedir que los usuarios sin privilegios puedan leer el archivo donde se almacenan las claves cifradas; otro método muy utilizado es el envejecimiento de contraseñas (aging password), que consiste en dar a la contraseña un tiempo de vida, transcurrido éste expira y se debe volver a cambiar; otro método es la utilización de claves de un solo uso, donde el usuario posee un pequeño dispositivo que le proporciona una secuencia de caracteres que deben ser digitados, junto con un PIN que el usuario debe mantener en secreto.

Es muy importante crear conciencia en todos los usuarios, la conveniencia de cambiar periódicamente sus contraseñas, mantenerlas en secreto y

modificarlas cuando se sospeche que alguien la conoce.
Amenaza
Rotación de personal, atacante interno.
Riesgo: Alto
Costo Asociado
La gran mayoría de los fraudes, robos, sabotajes o accidentes relacionados con sistemas informáticos, se presentan por personal que trabaja o ha trabajado con la empresa o institución afectada. Los motivos que llevan a una persona a convertirse en una amenaza para su propia organización, son diversos, en su gran mayoría son por inconformidad económica, mal ambiente laboral, inconformidad con el cargo, salida involuntaria de la empresa, etc.
Medidas de Contención
Para prevenir o minimizar los efectos de un atacante interno se deben seguir las siguientes recomendaciones: • A cada usuario se le debe asignar el mínimo de privilegios que necesita para desempeñar correctamente sus funciones. • Las actividades más delicadas dentro de las organizaciones, referentes a la seguridad (administración y control de los sistemas) deben ser realizadas por dos personas competentes, de forma tal que si alguno de ellos comete un error o intenta violar las políticas de seguridad, el otro pueda darse cuenta rápidamente y subsanarlo o evitarlo. También puede pasar que sí alguno de los responsables no está presente o incapacitado, el otro pueda seguir operando los sistemas normalmente. • Es recomendable realizar rotación de funciones y responsabilidades entre los responsables de los sistemas; puesto que en el caso que alguno abandone la organización, el otro pueda cubrir rápidamente sus responsabilidades y funciones, sin causar traumatismos en la organización.

Cuando un empleado abandone la organización, se debe cancelar inmediatamente el acceso a todos los recursos del sistema como cuentas de usuario, servicios de acceso remoto, unidades de red, cambio de claves del usuario y de su entorno.
Amenaza
Inserción e infectación de troyanos, virus, gusanos y otras amenazas.
Riesgo: Alto
Costo Asociado
La inutilización o trabajo inapropiado de los equipos de cómputo en las diferentes oficinas a causa de virus u otras infecciones, genera lentitud en los procesos de comercialización y venta de telefonía celular, represamiento en la entrega de informes, pérdidas económicas incalculables, etc. Más aún cuando se trata de los servidores de bases de datos, puesto que todas las oficinas a nivel nacional dependen del correcto funcionamiento de estos equipos.
Medidas de Contención
Se tienen instalados y actualizados antivirus en los diferentes equipos de cómputo. Se realizan frecuentes mantenimientos preventivos y se generan backups periódicamente a cada uno de los equipos. De igual forma, para aquellos equipos que son prioridad, se tienen habilitados equipos de contingencia listos para cambiarse, ante la presencia de un ataque o daño físico presentado.

3.3.2.2 Software que permite mantener la seguridad del Sistema

Existen en el mercado y en Internet una gran cantidad de herramientas que permiten mejorar la seguridad de la red y explorar los sistemas en busca de problemas o vulnerabilidades existentes. Entre ellas tenemos las siguientes:

- **Tripwire:** Es un comprobador de integridad para archivos y directorios de sistemas Unix, cuya función es comparar un conjunto de objetos previamente almacenados con una base de datos, y alerta al administrador al presentarse algún cambiado.

- **Tcp Wrappeers:** Permite definir una serie de redes o equipos autorizados para acceder a los servicios iniciados por ined, en los equipos de la red local. TcpWrappers le permite al administrador tener el control sobre las conexiones TCP que se realizan en el sistema.

- **Shadown Segurity Scanner (SSS):** Es un explorador de redes muy rápido, desarrollado para brindar seguridad y confiabilidad en la detección de un amplio rango de huecos de seguridad en los sistemas. Después de explorar el sistema SSS analiza los datos recopilados, localiza las vulnerabilidades o errores, y sugiere posibles métodos de solucionar los problemas. SSS se ejecuta sobre plataformas Windows y explora servidores sobre casi cualquier plataforma. Audita servicios como: FTP, SSH, Telnet, SMTP, DNS, Finger, http, POP3, IMAP, NetBios, NFS, NNTP, SNMP, Squid, servidores Proxy, LDAP, HTTPS, SSL, TCP/IP, UDP, entre otros.

- **Network Mapper (Nmap):** Explora rápidamente redes grandes, y determina cuales host están disponibles, qué servicios (puertos) están

abiertos, cuál sistema operativo y versión está corriendo, que tipo de filtrado de paquetes o Firewalls se están usando, entre otras muchas funciones.

- **Network Security Scanner (NSS):** Detecta automáticamente vulnerabilidades de seguridad en la red. Revisa la red contra todos los potenciales métodos que un hacker puede usar para atacarla, identifica huecos de seguridad e informa sobre las debilidades encontradas.

- **Scanlog:** Es una herramienta para detectar la exploración de puertos, y registra el evento usando syslog, es totalmente segura de usar. Si una dirección fuente envía múltiples paquetes a diferentes puertos en un corto tiempo, el suceso será registrado como una línea de alerta en los archivos de logs.

- **Network User Interface:** Suministra al administrador del sistema una poderosa herramienta gráfica para localizar, acceder, diagnosticar y administrar los recursos de la red.

3.3.3 Reuniones del comité de seguridad

El comité de seguridad programó reuniones generales cada semana y parciales cada tercer día, para ir analizando los riesgos y vulnerabilidades existentes y de igual forma proponer alternativas de solución. Una de ellas fue la implementación de capacitaciones en seguridad en cada una de las diferentes áreas de trabajo, tanto en la sede administrativa, como en las diferentes oficinas sucursales en todo el país.

3.3.4 Análisis de riesgo en los activos de la empresa CELTEL S.A.

El análisis de riesgo permite dar a conocer una serie de recomendaciones para prevenir la ocurrencia de tales amenazas o minimizar sus efectos en caso que se produzcan. Los mecanismos de seguridad se dividen en tres grupos: prevención, detección y recuperación.

- **Los mecanismos de prevención** son aquellos que aumentan la seguridad de un sistema, durante su funcionamiento normal, evitando la ocurrencia de violaciones de seguridad. CELTEL S.A. en el aspecto relacionado con acceso físico a implementado restricciones de acceso a diferentes áreas. En lo referente al hardware, se realiza mantenimiento a los equipos en forma periódica, se tienen equipos, discos duros, memorias, tarjetas, switches de respaldo para cuando alguno falle. En lo relacionado con el software y los datos, se realizan copias de seguridad frecuentes, se mantiene actualizado los antivirus y se utiliza cifrado de paquetes en la transmisión de datos.
- **Los mecanismos de detección** son aquellos que se utilizan para detectar violaciones de seguridad o intentos de violación. En la empresa CELTEL S.A. se utilizan algunos programas de auditoria como *tripwire*.
- **Los mecanismos de recuperación**, son aquellos que se aplican cuando se detecta que la violación al sistema se ha presentado y se desea retornarlo a su funcionamiento correcto. CELTEL S.A. mantiene actualizado los instaladores de sistema operativo y software de aplicación y de igual forma aumentó el periodo de generación de copias de seguridad en todos sus equipos.

Dentro de este último grupo, encontramos un subgrupo denominado mecanismos de análisis forense, el cuál tiene como objetivo no solo retornar al sistema a su modo de trabajo normal, sino identificar el alcance de la violación, las actividades de un intruso en el sistema y la puerta utilizada para vulnerar la seguridad del sistema.

Evitar un ataque, detectar un intento de violación o detectar una violación exitosa inmediatamente después de ocurrida, es mucho más productivo y menos comprometedor que tener que restaurar por completo el sistema.

3.3.5 Medidas de seguridad existentes en CELTEL S.A.

El departamento de sistemas, es consiente de las deficiencias en seguridad y la existencia de algunas vulnerabilidades en los sistemas de la empresa Celtel S.A. y como mecanismo de protección ha implementado los siguientes sistemas de protección:

- Firewall: Actúa como mecanismo de defensa, permitiendo o denegando las trasmisiones de una red a otra y evita que intrusos puedan acceder a la información que maneja la empresa; delimitando el perímetro de seguridad de la información dentro de la empresa.

- Servidor Proxy: Actúa como intermediario entre el programa cliente (Internet Explorer) y el servidor de datos al que se desea acceder. El servidor Proxy almacena de forma local las paginas más consultadas, para que al ser nuevamente solicitadas, el Proxy pueda servirla evitando así nuevamente el acceso remoto.

- Protocolo SSH: Se implementó este tipo de conexión remota segura en el servidor atlas y servidor ZEUS de la empresa, a través de la instalación del software de comunicación Open SSH_3.4.

3.4 DOCUMENTO

El documento que recopila la política de seguridad, debe ser claro, conciso y manejar un lenguaje poco técnico, para que pueda ser consultado y entendido por cualquier usuario de la empresa; también es importante actualizarlo permanentemente para que la política de seguridad no quede obsoleta en pocos años.

3.4.1 Objetivos y ámbito

Las políticas de seguridad informática definidas en el presente manual, tienen como finalidad salvaguardar la información y demás activos que posee la empresa CELTEL S.A. para lo cual es necesario:

- Incentivar en el personal administrativo y operativo de la empresa la importancia de proteger la información, pues es el recurso más valioso con el que cuenta la organización.
- Definir políticas de seguridad encaminadas a proteger los activos de la empresa, especificando los deberes, derechos y responsabilidades de los usuarios, de acuerdo al área de trabajo en la cual se desempeñan. Buscando el mayor nivel de confiabilidad de la información.
- Desarrollar normas y procedimientos para la adecuada administración y mantenimiento de los servidores.

- Crear hábitos de seguridad tanto a los usuarios autorizados en los servidores de datos, como a los usuarios de las estaciones de trabajo de cada departamento (contabilidad, sistemas, inventarios, etc.).

El ámbito de la política de seguridad es aplicable al área administrativa, operativa y comercial de la empresa CELTEL S.A. cuya sede principal se encuentra ubicada en Sangil (Santander).

3.4.2 Política de seguridad física

El comité de seguridad es el encargado de gestionar la adecuación de las instalaciones, donde se encuentran los servidores y los equipos de cómputo, con el objetivo de garantizar la protección contra amenazas ambientales, fluctuaciones de corriente eléctrica, accesos no autorizados, perdidas de información, etc.

Procedimientos:

- Se debe adquirir otra UPS APC-Smart-UPS 3000 para el Servidor Proxy y el Firewall y 3 UPS Power Back 600 para la estaciones de trabajo de inventarios y contabilidad, que mantengan el nivel de carga adecuada a las exigencias de los servidores y/o equipos de computo que lo requieran. De igual forma, es necesario contar con un sistema de regulación de voltaje, para la protección de los equipos de cómputo; ante las variaciones presentadas en el suministro de energía.
- Realizar mantenimiento trimestralmente y en forma adecuada al sistema de aire acondicionado, para brindar una temperatura acorde a los requerimientos de los servidores y equipos de cómputo.
- El cuarto de equipos debe estar aislada de posibles fuentes de inundación, fuego, humo o polvo excesivo.

- Se debe contar con un sistema de alarma contra incendios y con la cantidad de extintores adecuados para contrarrestar todo tipo de conflagración; los cuales deben estar ubicados estratégicamente, para su fácil visibilidad y acceso.
- Generar periódicamente copias de seguridad, que permitan la restauración del sistema en caso de presentarse pérdida de información. Las copias deben almacenarse en sitios seguros, con acceso restringido y en localidades diferentes.
- Se deben mantener sistemas de respaldo o contingencia para los servidores o equipos de cómputo que presentan alta disponibilidad de servicio y que son fundamentales, para el desempeño normal de las actividades de la empresa.
- El cuarto de equipos donde se encuentran los servidores debe tener acceso restringido al personal no autorizado y manejar diferentes esquemas de seguridad como: puertas con cerraduras adecuadas, cámaras de video, censores de movimiento, etc.
- El personal externo, encargado del mantenimiento de los servidores debe identificarse previamente y portar el carnet de la institución a la que pertenece.
- Cuando se trasladen copias de seguridad, listados, partes de equipos, o cualquier otro elemento relevante a la sala de servidores, debe realizarse solo por personal autorizado, además debe registrarse por escrito en un formato previamente establecido; el cuál debe tener: el nombre e identificación de la persona que lo retiró, dependencia, causa y características del material retirado.
- El ingreso al cuarto de equipos con comidas, bebidas, líquidos de diferentes tipos, paquetes, morrales, bolsos, medios magnéticos, etc. debe estar prohibido. De igual forma en las estaciones de trabajo esta prohibido el acceso de comidas, bebidas y líquidos de cualquier tipo.

3.4.3 Política de seguridad de cuentas de usuario

Las cuentas de usuario son creadas por el administrador del sistema y serán otorgados sólo a usuarios autorizados y de acuerdo a las funciones realizadas.

Procedimientos:

- La solicitud para la creación de una nueva cuenta de usuario se debe hacer por escrito, mediante un formulario en el que se registra la información personal del usuario, la descripción general de la función a realizar, la dependencia en la que labora, la firma del jefe de la dependencia o coordinador de la oficina.
- Los privilegios asignados a cada cuenta de usuario, serán estrictamente los necesarios para poder cumplir con sus labores y funciones dentro de la empresa.
- Cuando un usuario se retira de la empresa, se bloquea inmediatamente su cuenta de usuario y se cambian las cuentas y contraseñas de su entorno de trabajo.
- Cada cuenta de usuario es personal y cada uno es responsable del buen o mal manejo que se realice con ella. No se permiten cuentas compartidas.
- Las cuentas inactivas por mucho tiempo, son bloqueadas automáticamente por el sistema.

3.4.4 Políticas de contraseñas

Cada cuenta de usuario tiene asociada una contraseña única. La cual debe tener como mínimo 6 caracteres y debe estar compuesta por una combinación da caracteres numéricos, alfanuméricos y/o símbolos.

Procedimientos

- La contraseña de cada usuario es personal, no debe ser prestada bajo ninguna circunstancia. En caso de sospechar que otro usuario conoce su contraseña, se debe reportar inmediatamente al administrador del sistema y solicitar cambio de contraseña.
- Las contraseñas elegidas por los usuarios, no deben ser palabras de diccionario, fechas especiales, nombres de personas. Se deben utilizar combinaciones de minúsculas y mayúsculas, números mezclados con textos, símbolos especiales como: $, &, #, ¡, [, _, etc.
- Se deben implementar sistemas de protección, como el oscurecimiento de contraseñas (Shadow Password) y el envejecimiento de contraseñas (Aging Password).
- Se deben cambiar periódicamente las contraseñas de los usuarios, especialmente las que se consideren más vulnerables a ataques de cifrado o los que presentan mayor riesgo, de acuerdo a las funciones realizadas.

3.4.5 Políticas de uso adecuado de los recursos informáticos

Responsabilidades del administrador de la seguridad informática.

- Crear los usuarios que están autorizados para acceder a los recursos informáticos de la empresa, según los lineamientos y procedimientos definidos para la creación de usuario.
- Implementar procesos de autenticación de usuarios, para controlar el acceso a los sistemas de información.

- Auditar periódicamente el sistema de contraseñas, mediante algún programa crackeador disponible, con el objetivo de encontrar passwords débiles y en consecuencia dar solución inmediata a la debilidad presentada.
- Explorar periódicamente los servidores con herramientas tipo scanner, con el objetivo de encontrar vulnerabilidades, puertos o servicios abiertos que no son necesarios para el correcto desempeño del servidor.
- Verificar continuamente la integridad del sistema, mediante herramientas como Tripwire y el acceso a los servicios de las maquinas, con herramientas como TCP Wrappers.
- Documentar los procedimientos realizados en los servidores y demás recursos informáticos, para tener un manual o guía cuando se presente una situación similar.
- Promover el uso de técnicas para la protección de los datos, como las herramientas de cifrado, instalación y configuración de Firewalls, sistemas de detección de intrusos, etc.
- Coordinar la Instalación y configuración del software y hardware necesario para el desempeño de las actividades propias de cada usuario.
- Brindar soporte técnico a los usuarios del sistema, dando soluciones oportunas y capacitando para evitar las vulnerabilidades que puedan ocasionarse.
- Implementar procedimientos de monitoreo de conexiones activas, para detectar cuando un usuario permanece por largo tiempo en estado de inactividad, en consecuencia, cerrar la conexión y generar un log con el acontecimiento presentado.
- Definir políticas de copias de seguridad, en las que se especifique la información que debe respaldarse y con que periodicidad, los medios de respaldo a utilizar, el lugar donde se almacene los backups, el proceso para realizar la restauración de la información y la forma de crear la rotulación para las copias de seguridad.

Responsabilidades de los usuarios del sistema

- Cambiar periódicamente las claves de acceso al sistema; asignando combinaciones de números, letras, minúsculas, mayúsculas y símbolos, o utilizando software para la creación de contraseñas; como *password depot***.**
- No compartir la clave bajo ninguna circunstancia, puesto que la cuenta de un usuario es personal e intransferible. En caso de sospechar que otra persona sabe la clave, se debe cambiar inmediatamente e informar al administrador del sistema.
- Cada usuario es responsable de su cuenta y password respectivo y de los procesos que puedan realizarse, en las aplicaciones que posee la empresa, mediante la utilización de su cuenta de usuario.
- Cuando un usuario se ausente momentáneamente de su estación de trabajo, debe cerrar todas las sesiones abiertas en el servidor.
- Cuando un usuario detecte anomalías o vulnerabilidades, que amenacen de alguna forma la seguridad de los recursos informáticos, la debe reportar inmediatamente al administrador del sistema.
- No esta permitido el uso e instalación de software y aplicativos, diferentes a los autorizados por el administrador del sistema.
- Los usuarios deben conocer, aceptar y seguir las normas, procedimientos y políticas implementadas para la utilización de los recursos informáticos.

3.5 IMPLANTACIÓN DE LA POLITICA DE SEGURIDAD

Todas las normas y procedimientos consignados en el manual de seguridad, las responsabilidades y deberes de los usuarios del sistema, así como las

sanciones que se impondrán por el incumplimiento de las mismas, deben ser comunicadas de manera clara y precisa a todo el personal, en las áreas de aplicación definidas.

Procedimientos:

- Realizar reuniones informativas, en cada una de las áreas de aplicación definidas.
- Mediante el servicio de correo electrónico se informará a cada uno de los usuarios, adjuntando el archivo de la política de seguridad.
- Publicar la política de seguridad en la Intranet de la empresa.
- Informar a los usuarios, las modificaciones realizadas a la política de seguridad, enviando correo electrónico a cada uno de ellos.

El desconocimiento de las normas y/o modificaciones a las mismas, hace más vulnerable la seguridad de cualquier sistema informático.

4. CONCLUSIONES

Este capítulo presenta las conclusiones obtenidas, durante el proceso de elaboración de la política de seguridad informática para la empresa Celulares y Comunicaciones CELTEL S.A.

- Las redes de datos han contribuido significativamente al comercio electrónico, el intercambio de información, a hacer más eficientes los procesos y minimizar el tiempo de ejecución de los mismos, sin importar las distancias; por ende cada día aumenta significativamente el número de usuarios en la red y de igual forma crece la preocupación de los administradores de sistemas en mejorar la seguridad de su entorno laboral.

- La información es el recursos más valioso que poseen las empresas y el más difícil de recuperar; es el principal activo que debe salvaguardar cualquier entidad pública o privada, educativa o comercial; garantizando su integridad, confidencialidad y disponibilidad. Pero también crece significativamente el número de atacantes que buscan aprovechar las vulnerabilidades que tienen las empresas para extraerla, con el propósito de divulgarla, venderla, usarla para beneficio propio, destruirla, etc. Dentro de éste grupo de personas potencialmente interesadas en atacar nuestro sistema y quizás uno de los más peligrosos, se encuentran los antiguos empleados, especialmente los que no abandonaron el cargo por voluntad propia.

- La política de seguridad se fundamenta en los riesgos y vulnerabilidades detectadas sobre los activos organizativos, y las medidas de contención adaptadas para minimizar el impacto de dichos riesgos en la seguridad del sistema.

- Es importante crear conciencia en todo el personal, la importancia de su papel en la política de seguridad del entorno; y aunque los riesgos no se pueden eliminar por completo, lo que se puede hacer es minimizarlos, administrarlos y reducir el impacto que puedan generar.

- Una política de seguridad se encuentra bien implantada, cuando es consecuente con los objetivos de la empresa, brinda seguridad a todos los procesos y garantiza una gestión inteligente de los riesgos.

- Planificar, analizar y diseñar una eficiente política de seguridad informática, le permite a las empresas ejecutar las acciones necesarias para minimizar el impacto que produce un ataque informático; también es una herramienta muy importante para la alta gerencia en la toma de decisiones y crea conciencia del papel que cumplen los empleados y directivos en preservar la seguridad e integridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

RICO ARENAS, Rocío Carolina. Seguridad informática, sus implicaciones, su importancia en el diseño de las redes de datos y su aplicabilidad en los servidores de la red Lan de la universidad industrial de Santander. Bucaramanga, 2003. 115 p.

GUTIÉRREZ PICÓN, María Eugenia. Diseño de plan estratégico de los sistemas de información de la Fundación Oftalmológica de Santander Clínica Carlos Ardila Lule FOSCAL. Bucaramanga, Junio de 2005. 80 p.

PARRA ORTEGA, Carlos Arturo y otro .Detección de intrusos en redes utilizando SNORT. Bucaramanga, 2003. 33 p.

LUCENA LOPEZ, Manuel José. Criptografía y seguridad en computadores. [OnLine]. Universidad de Jaén. Disponible en Internet:
< http://wwwdi.ujaen.es/~mlucena/lcripto.html >

3COM. Productos y Servicios [OnLine] < http://lat.3com.com/lat/

VILLALÓN HUERTA, Antonio. Seguridad en Linux y Redes. Febrero de 2006. [OnLine]. Disponible en Internet:
< http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node72.html >