PROPUESTA DE DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS INSTITUCIONAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

CARLOS ALBERTO PARRA CORREA

Trabajo de investigación como requisito para optar al título de Magíster en Ingenierías

Director
Ing. Hernán Porras Díaz, M.Sc., Ph. D.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS FISICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2006

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del director

_____
Firma del Jurado

_____
Firma del Jurado

Bucaramanga, septiembre 18 de 2006

A Dios, quien me sostuvo a pesar de todas las dificultades en el camino, a mi Maestro B:. O:. guía y luz de mi existencia.

A mis padres Luis Alberto y María Esther por su continuo apoyo.

A mi esposa Myriam por darme la alegría del calor de un bello hogar y esos hermosos frutos que son motivo de mi más alta esperanza e inspiración: Carlos David, Angela Paula y nuestro próximo bebé.

Carlos Alberto

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

RESUMEN

TÍTULO: PROPUESTA DE DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS INSTITUCIONAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER.*

AUTOR: CARLOS ALBERTO PARRA CORREA**

PALABRAS CLAVES: amenazas, seguridad Informática, auditoria, análisis de riesgos, prospectiva, modelos de seguridad informática, políticas de seguridad informática, estándares de seguridad informática, procedimientos de seguridad informática

DESCRIPCIÓN O CONTENIDO: Con la aparición y masificación del uso de las redes informáticas y en especial de la red de redes Internet, las organizaciones abrieron los ojos y notaron enormes ventajas y posibilidades, convirtiendo a la información procesada, almacenada o transmitida en un activo de suma importancia para cualquier organización. Es así, como las universidades y en particular la Universidad Industrial de Santander decidieron acceder a estas tecnologías, porque les permitía una ubicación estratégica, es decir, estar en todas partes, lo mismo que la posibilidad de intercambiar conocimientos tecnológicos, tanto a nivel local como mundial. Paralelamente a este mundo de oportunidades surgieron individuos que realizaban actividades ilegales que tenían como objetivo irrumpir en flujos de información privados y confidenciales, haciendo que las redes y en particular Internet se convirtiera en un entorno inseguro para cualquier organización.

La Universidad Industrial de Santander no ha sido ajena a esta problemática, ya que también ha sido blanco de ataques y ha presentado debilidades potenciales con respecto a su seguridad informática. Situación que ha originado esfuerzos en procura de investigar acerca de la posibilidad de hallar soluciones integradas y respaldadas por la misma institución, obteniéndose como resultado un modelo de seguridad informática para la UIS. Dicho modelo fue obtenido a partir de la búsqueda y recolección de información relacionada con las amenazas informáticas más importantes que pudieran afectar la UIS.

Respecto al análisis de riesgos se utilizó una metodología que no había sido empleado antes denominada “análisis estructural para estudios prospectivos”, la cual condujo a la obtención de las variables claves del sistema, permitiendo valorar nivel de riesgo informático. Se indagó además acerca de los modelos de seguridad más importantes del mundo con el fin de extractar los lineamientos

---

* Trabajo de investigación

** Ingenierías Físico-Mecánicas. Maestría en Informática Ing. Hernán Porras Díaz, M.Sc., Ph. D.

básicos que debe soportar un adecuado modelo de seguridad informática, el cual se compone de políticas, estándares y procedimientos en constante ciclo de mejoramiento.

ABSTRACT

TITLE: PROPOSAL ABOUT THE DESIGN OF AN INFORMATIC SECURITY MODEL FOR THE INSTITUTIONAL DATA NETWORK OF SANTANDER INDUSTRIAL UNIVERSITY*

AUTHOR: CARLOS ALBERTO PARRA CORREA**

KEYWORDS: threatens, informatic security, audits, risk analysis, prospective, informatic security model, informatic security policies, informatic security standards, informatic security proceedings.

DESCRIPTION OR CONTENT: The surge and massification of informatic network using, and especially, the internet net of networks make the organizations acknowledge the huge advantages and possibilities by rendering the stored, transmitted and processed data an outstanding asset for any organization. Therefore, universities particularly Industrial University of Santander (I.U.S) decided to obtain these technologies, since it allows them a strategic position, it means, being in every place as well as the possibility of exchanging technological knowledge both at a local level and around the world. Simultaneously to this collection of opportunities some people that do illegal activities showep up who aims at breaching private and confidential data diagrams by making, that networks and particulary the internet, became and insecure environment for every organization.

I.U.S has been affected by that, since it has been a target for attacks, and it has potential frails related to the informatic security. That situation has originated the gathering of efforts to investigate about the possibility of finding integrated solutions supported by the institution. As a result an informatic security model was conceived for I.U.S. That model was achieved by the searching and collection of information related to the most important threatens that might affect I.U.S.

For the risk analysis a methodology which hasn´t used before was used. It´s called “structural analysis for the prospective studies” which leads to the obtention of key variables for the system, allowing to asses the informatic risk level. Besides, the most important security models in the world were investigated in order to draw the basic guidelines that have to support a proper informatic security model which comprises policies, standards and proceeding which are increasingly bettering.

* Work of investigation

** Physical-Mechanical Engineering School. Informatic Master. Hernán Porras Díaz, M.Sc., Ph. D.

INTRODUCCION

Las redes informáticas y en especial la red de redes Internet, provocaron que las organizaciones aprovecharan las enormes ventajas y posibilidades, convirtiendo a la información procesada, almacenada o transmitida en un activo muy importante. Por lo tanto las universidades y en particular la Universidad Industrial de Santander no se quedaron atrás decidiendo también emplear estas plataformas tecnológicas, porque les permitía una ubicación estratégica, es decir, estar en todas partes, como también la posibilidad de intercambiar conocimientos tecnológicos, tanto a nivel local como mundial. Desafortunadamente surgieron individuos que efectuaban actividades ilegales, que les permitieron irrumpir en flujos de información privados y confidenciales, convirtiendo las redes y en particular Internet en entornos inseguros para cualquier organización. La Universidad Industrial de Santander no ha sido ajena a esta problemática, ya que también ha sido objeto de ataques y ha presentado debilidades potenciales con respecto a su seguridad informática, intentando contrarrestar esta situación con soluciones parciales no muy efectivas, motivo por el cual se orientaron esfuerzos en procura de investigar acerca de la posibilidad de hallar soluciones integradoras que se transformaran en un modelo de seguridad informática adecuado para la UIS. Es así como se efectuó la búsqueda y recolección de información relacionada con las amenazas informáticas que pudieran afectar la UIS, valorando el riesgo informático, empleando una metodología prospectiva denominada “análisis estructural de variables” y estudiando los modelos de seguridad más importantes a nivel mundial, con el fin de fundamentar los pilares fundamentales que permitieran proponer un modelo de seguridad informática.

1. SEGURIDAD INFORMÁTICA

1.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Con la aparición y masificación del uso de Internet las organizaciones abrieron los ojos y notaron enormes ventajas y oportunidades tales como: ubicación estratégica, es decir, estar en todas partes, lo mismo que la posibilidad de intercambiar conocimientos tecnológicos en tiempo real, tanto a nivel local como mundial. Además de su escalabilidad, es decir su capacidad de adaptación a nuevos entornos tecnológicos y por último su accesibilidad en costos. Ante estas ventajas y oportunidades estratégicas, las organizaciones han buscado conectar para sus negocios, clientes, proveedores, ubicaciones remotas, sucursales y empleados móviles directamente en línea a la red de la empresa, sin embargo, paralelamente a este mundo de oportunidades surgieron individuos que realizaban actividades ilegales que tenían como objetivo irrumpir en flujos de información privados y confidenciales, haciendo que Internet se convirtiera en un entorno inseguro para cualquier organización.

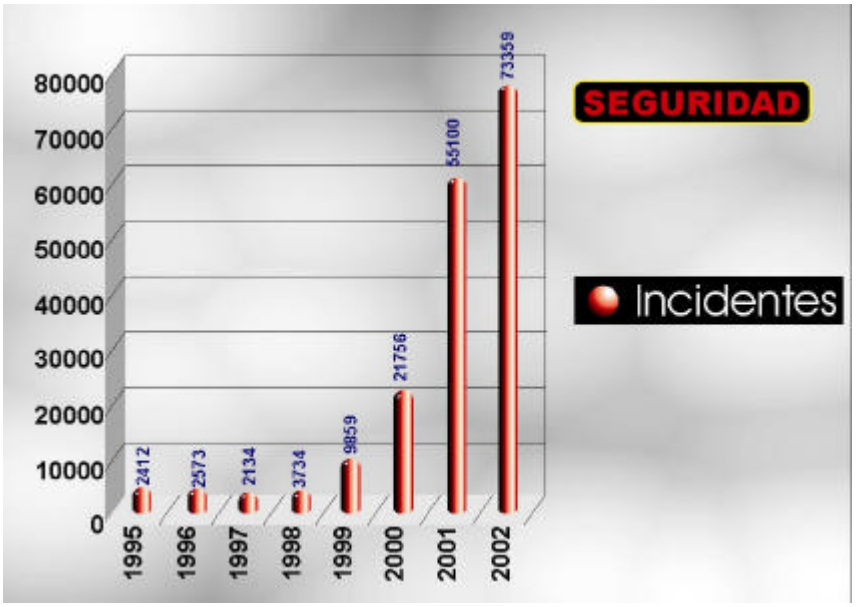
Si revisamos estadísticas de seguridad en cómputo indican que cerca del 80% de los fraudes relacionados con las computadoras provienen de los usuarios internos, por esto las intranets son las más vulnerables a ataques de ésta índole.

Según el CSI (Computer security institute) de San Francisco el 90 % de las empresas entrevistadas detectaron ataques a sus computadoras, el 70 % reportó que los más comunes fueron virus, robo de laptops y ataques de abuso de la red de sus empleados.[1]

El CERT en la reunión de primavera del 2003 reportó el siguiente informe acerca de incidentes informáticos en los Estados Unidos: (Figura 1).

[1] Información basada en http://www.corporate-intranet.com/treasury/articles/art04.html, http://www.cert.com, http://www.gocsi.com/prelea_000321.htm

Figura 1. Variación Incidentes de Seguridad



Fuente: CANO, J. (2002) *Estado de la Seguridad Informática en Colombia*. Revista SISTEMAS. Asociación Colombiana de Ingenieros de Sistemas – ACIS. No.82. Julio- Septiembre

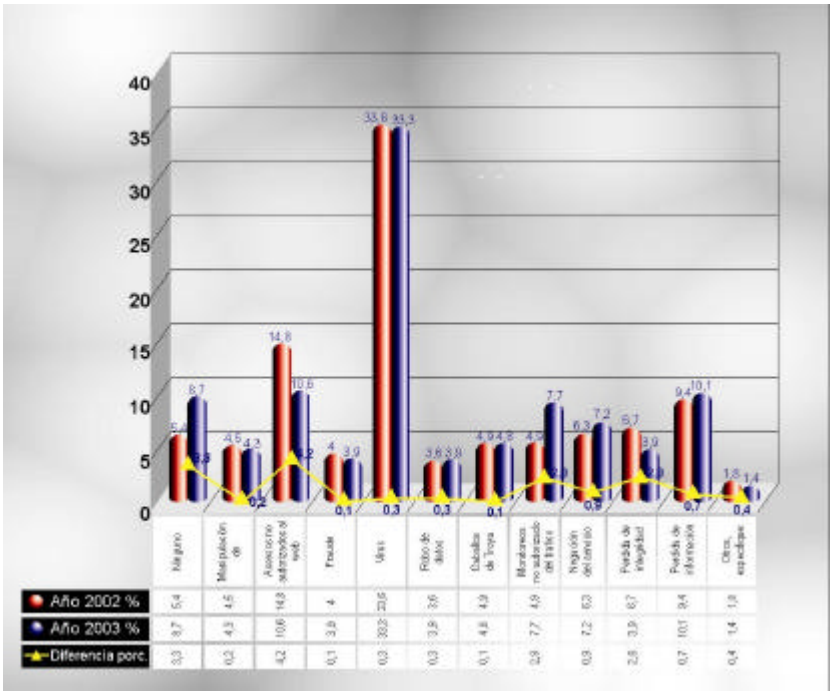
El diagnóstico de seguridad de delitos por computadores realizado en el 2002 en los Estados Unidos por el Instituto Nacional Computacional en conjunto con el F.B.I arrojaron los siguientes resultados: Del 100% de empresas que contestaron se tiene que:

- 62% sufrieron violaciones a la seguridad informática.
- 30% reportó penetración por hackers externos.
- 57% reportó intrusión en conexiones de internet.
- 32% reportó negación de servicios por ataques masivos.
- 19% experimentó sabotaje en redes de datos.
- 14% reportó ser víctima de fraude financiero.
- 90% tuvo incidentes de contaminación por virus.
- 55% reportó accesos no autorizados de empleados.
- 97% reportó abuso interno de privilegios de internet.
- 69% reportó pérdidas y robos de laptops.
- 26% mencionó robo de información de su propiedad.
- 32% reportó los incidentes a las autoridades de justicia.

Las pérdidas estimadas en 3 años consecutivos superaron los 100 millones de dólares.

En Colombia los reportes de violaciones de seguridad en los últimos dos años muestran la siguiente tendencia: (Figura 2).

Figura 2. Violaciones de Seguridad Informática en Colombia.



Fuente: III Encuesta Nacional de Seguridad Informática ACIS 2003.

Analizando los informes anteriores, tanto a nivel mundial como local, se observa un incremento acelerado de factores que afectan la seguridad de la información de las organizaciones, provocando la necesidad de investigación tanto de empresas tecnológicas como de la academia, conformando lo que hoy en día se conoce como seguridad informática.

1.2 RESEÑA HISTÓRICA – GENERALIDADES

Algunos hechos que han marcado la seguridad informática en forma significativa a nivel mundial y local son los siguientes:

En 1949, el matemático estadounidense de origen húngaro John Von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en la década de 1950 en los Bell Laboratories, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él. En 1983, el ingeniero eléctrico

estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término "virus" para describir un programa informático que se reproduce a sí mismo.[2]

En 1977 Ron Rivest, uno de los fundadores de RSA Data Systems, creó un sistema de encriptación de clave pública que se utiliza en una gran cantidad de sistemas operativos y programas Internet. Su desafío llamado RSA –129 retó a cualquiera que quisiera romper un mensaje específico encriptado con su clave numérica de 129 dígitos. Rivest creyó que se tardaría algo así como 40 cuatrillones de años para poder hacerlo. En 1994 un equipo organizado por el estudiante del MIT Derek Atkins utilizó simultáneamente 1600 computadoras conectados a Internet para romper el código en un período no consecutivo de ocho meses. Las actuales implementaciones RSA emplean claves mucho más largas.[3]

En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos. El virus llamado Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

Actualmente el medio de propagación de virus más extendido es Internet, en concreto mediante archivos adjuntos al correo electrónico, que se activan una vez que se abre el mensaje o se ejecutan aplicaciones o se cargan documentos que lo acompañan.[4]

En 1987, el infausto gusano de Internet desarrollado por un estudiante de Cornell, se duplicaba a sí mismo por Internet, e infectaba a las computadoras con copias de sí mismo hasta que las dejaba fuera de combate.[5]

En el año de 1994, un experto en computadoras ruso, junto con algunos cómplices efectuaron una serie de incursiones encubiertas a los mainframes del Citibank establecidos en Nueva York. Los rusos lograron transferir por vía electrónica 11 millones de dólares a cuentas bancarias en Finlandia, Israel y California.[6]

---

[2] 1993-2003 Microsoft Corporation.
[3] SHELDON, Tom. Manual de Seguridad de Windows NT, 1 ed. Madrid: McGrawHill, 1997. p.21.
[4] 1993-2003 Microsoft Corporation.
[5] SHELDON, Tom. Manual de Seguridad de Windows NT, 1 ed. Madrid: McGrawHill, 1997. p.20.
[6] CLARK, David Leon. Guía para el Administrador de Redes Virtuales. 1 ed. México,D.F: McGrawHill, 2000. p. 81.

En este mismo año, Kevin Mitnick un pirata informático profesional que había sido arrestado por piratear sistemas telefónicos y computadoras corporativas, robó 20.000 números de tarjetas de crédito a un proveedor de servicios de Internet, fue detectado sólo cuando al proveedor le informó del hecho un soplón. También Mitnick violó el centro de supercomputación de San Diego saltándose un cortafuegos mediante el uso de una sesión de comunicaciones TCP/IP legítima. [7]

Hacia 1998, un grupo de hackers obtuvo números telefónicos privados e información de crédito de consumidor de redes privadas operadas por separado por Service Bureau Corporation (SBC), GTE, Macintosh y Sprint. En el proceso, estropearon las redes causando daños por 500 mil dólares. El F.B.I obtuvo una pista cuando los intrusos desviaron llamadas de sus centros hacía líneas de charla de sexo en Hong Kong y Moldavia. Lo que más preocupó a las empresas transportadoras comunes y al F.B.I fue su capacidad para obtener acceso y control de programas centrales, conocido como acceso raíz. Las agencias de servicio aprendieron que aunque los cortafuegos son efectivos, no son impenetrables.

Uno de los ataques más osados al pentágono comprendió el uso de los llamados programas software husmeador. Los hackers agregaron de manera clandestina "husmeadores" a dispositivos de red como enrutadores para monitorear información a medida que fluía por la red. Una de las instalaciones del comando superior y de investigación de control de la fuerza aérea de Estados Unidos, el laboratorio de Roma, encontró este problema en su conexión a Internet. Los hackers lograron detectar información mientras pasaba por los conmutadores de datos para obtener las contraseñas que se utilizaban para obtener acceso a la red interna de Roma. La red se enlazaba con sitios web internacionales. Una vez que estuvieron dentro, los hackers robaron investigaciones tácticas y de inteligencia artificial.

De acuerdo con el London Times, las instituciones financieras afectadas incluyendo el Banco de Londres, han llegado a pagar a los hackers más de medio millón de dólares por mantener el silencio en cuanto a los robos por computadora. Estas instituciones están utilizando una especie de chantaje inverso para evitar que los hackers hablen a los medios masivos de comunicación. Al parecer, estas medidas les garantizan evitar temores de sus clientes y autoridades de un ataque que haya tenido éxito.

En 1996, la Sociedad Estadounidense para la Seguridad Industrial estimó que los crímenes de alta tecnología les estaban costando a las empresas hasta 63 mil millones de dólares cada año. De manera sorprendente, en un desarrollo relacionado, las empresas pagan millones de dólares cada año a los hackers para

[7] SHELDON, Tom. Manual de Seguridad de Windows NT, 1 ed. Madrid: McGrawHill, 1997. p.20.

que mantengan la boca cerrada en cuanto a su éxito, en especial las empresas en que se incluye la seguridad de red como una garantía de servicio.

Otros estudios han demostrado que el costo de un plan efectivo de seguridad de red para una empresa con una LAN de 50 estaciones de trabajo y un sitio web podría ser de hasta 100 mil dólares. Los cortafuegos por sí solos pueden aumentar hasta 15 mil dólares por sitio.

El gobierno federal estadounidense ha colocado claramente a la seguridad de computadoras como alta prioridad. El F.B.I, la CIA y la NSA tienen pequeñas unidades operativas dedicadas a combatir problemas y crímenes de seguridad en computadoras.[8]

Revisando el entorno local, no ha estado ajeno a esta situación como lo demuestra la encuesta hecha en el 2003 por la Asociación Nacional de Ingenieros de Sistemas (ACIS) (Figura 2), allí se observa que también las organizaciones Colombianas han sido afectadas por virus, accesos no autorizados, fraudes, entre otros.

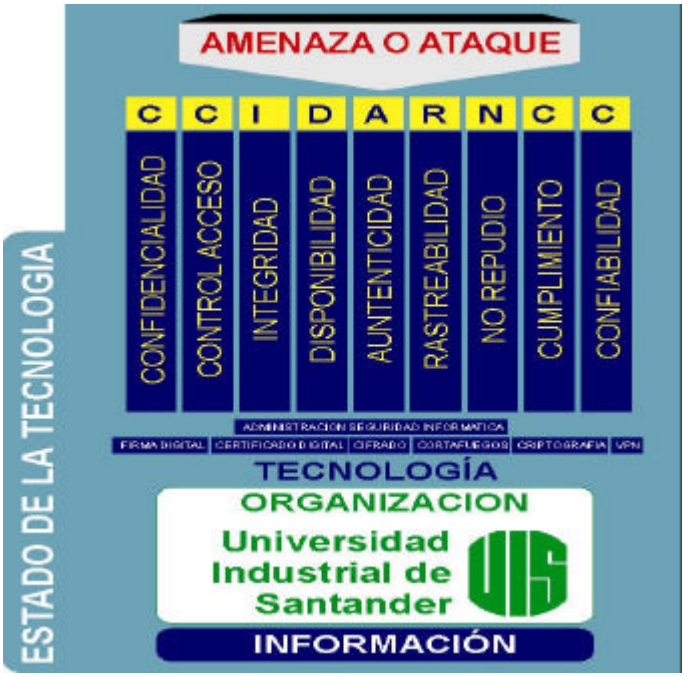
1.3 ESTADO DE LA TECNOLOGIA

Revisando el estado de la tecnología respecto a la seguridad informática se puede explicar mediante la figura 3 los principales ingredientes de la seguridad informática:

1.3.1 Amenaza. Se refiere a cualquier hecho natural o maniobra de tipo técnico o humana que puede modificar, interrumpir, interceptar o destruir la información de una organización. Existen diversos tipos de clasificaciones respecto a las amenazas informáticas, las cuales guardan alguna relación unas con otras, como se muestra en la figura 4, en la cual los diferentes colores mostrados en cada ítem, resaltan la relación entre las diferentes clasificaciones.

[8] CLARK, David Leon. Guía para el Administrador de Redes Virtuales. 1 ed. México,D.F: McGrawHill, 2000. p. 80-83.

Figura 3. Estado de la Tecnología



Fuente: Autor del proyecto.

De acuerdo al área donde se produzcan las amenazas se pueden clasificar en:

- Amenazas externas: Se originan fuera de la organización dentro de las cuales podemos encontrar los virus, gusanos, caballos de Troya, intentos de ataques de piratas informáticos, retaliaciones de ex-empleados o espionaje industrial.

- Amenazas internas: Son las que provienen del interior de la organización y pueden ser muy costosas debido a que el infractor por ejemplo un empleado descontento conoce muy bien la entidad objeto de ataque, tiene mayor capacidad de movilidad dentro de la misma, por lo tanto tiene mayor acceso y perspicacia para saber donde reside la información sensible e importante. Las amenazas internas también incluyen el uso indebido del acceso a Internet por parte de los empleados, así como los problemas que podrían ocasionar los empleados al enviar y revisar el material ofensivo a través de Internet.

Cuando la amenaza ya sea externa o interna se hace efectiva, se convierte en un ataque y estos pueden presentar efectos tanto activos como pasivos:

- Ataques Pasivos: son aquellos en los cuales el atacante recopila información sin que nadie de la organización sepa que se está produciendo. Tiene como objetivo la interceptación y el análisis de tráfico. Dentro de las técnicas más sutiles para obtener información se tienen:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los periodos de actividad.

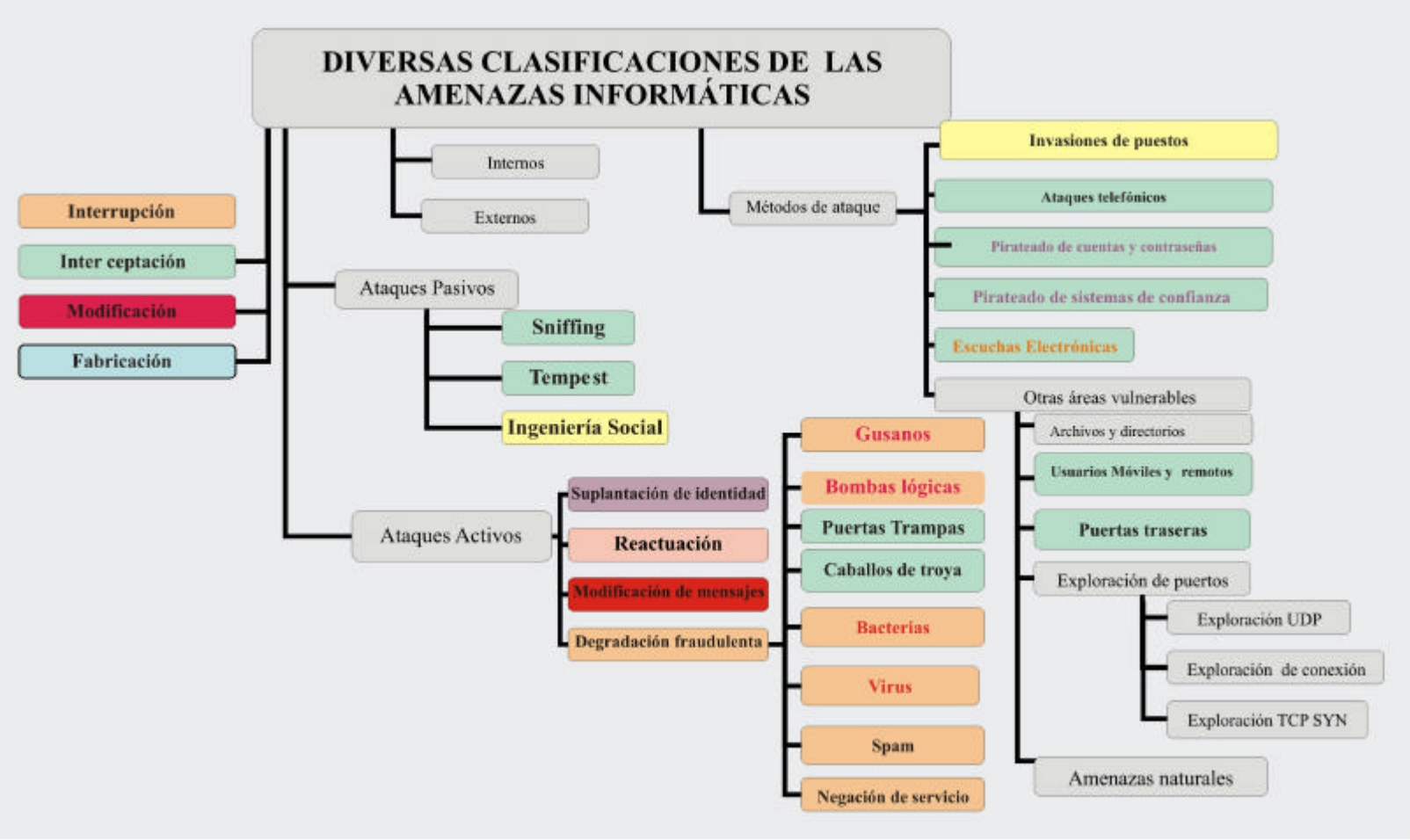
- Son ejemplos de estos ataques las escuchas y los pinchazos electrónicos (sniffing), tempest, lo mismo que ataques propiciados por la llamada ingeniería social, cuyas características se exponen a continuación:

- **Sniffing**: un sniffer es un programa que permite escuchar o monitorizar todo el tráfico de la red, puede colocarse en una estación de trabajo de la LAN, en un gateway o en un router. El sniffer va leyendo los mensajes que atraviesan la estación de trabajo, gateway o router donde esta instalado y graba la información en un fichero. Esto es posible porque la mayoría de las tarjetas de red ethernet tienen un modo llamado promiscuo, que les permite aceptar todos los datos de la red. En los primeros mensajes de conexión se encuentran los passwords sin cifrar.

- **Tempest:** todo equipo electrónico realiza emanaciones eléctricas y magnéticas. Es posible captar estas emanaciones y de ellas obtener información, esta tecnología es utilizada por agencias gubernamentales. Actualmente se fabrican equipos con filtro anti tempest.

- **Ingeniería Social:** mediante esta denominación no se pretende entrar en controversia con otras ramas del saber en donde su definición varía totalmente, sólo que en seguridad informática la “ingeniería social” se ha utilizado para denominar una serie de técnicas sicológicas que pueden permitir la obtención de información de manera engañosa o fraudulenta. Es el arte de convencer a la gente de entregar información sensible, como claves de acceso, y de esta forma colaborarle al atacante quien se hace pasar generalmente por el administrador de la red. Es altamente efectiva y difícil de controlar (Educación de usuarios).

Figura 4. Diversas Clasificaciones de las Amenazas Informáticas.



Fuente: Autor del proyecto.

- Ataques Activos: se refiere a modificaciones del flujo de datos que el atacante propicia en los datos almacenados o transmitidos. Estos cambios pueden consistir en el borrado, alteración, el retraso o interrupción en las transmisiones. Son difíciles de detectar, porque suelen camuflarse como eventos accidentales en la organización. Pueden dividirse en cuatro categorías:

· **Suplantación de Identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo secuencias se autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, esto es posible al sustraer la contraseña de acceso a una cuenta.

· **Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

· **Modificación de Mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje " Consigne 10 millones de pesos en la cuenta X" pudiera modificarse por " Consigne 10 millones de pesos en la cuenta Y".

· **Degradación fraudulenta del servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o podría interrumpir el servicio de una red inundándola con mensajes triviales. Entre estos ataques se encuentran los de negación de servicio, consistentes en paralizar temporalmente el servicio de un servidor que puede ser de correo, Web, FTP, etc.

Son ejemplos de ataques activos los siguientes:

1. Gusanos (Worms). Estas piezas de código se propagan por sus propios medios, absorbiendo en forma creciente recursos del sistema, hasta saturarlos causando efectos dañinos como el bloqueo a los sistemas. Son ejemplos de estos:

MELISSA: cuya propagación se hacía a través de correo electrónico.
NIMDA: consumía gran parte del canal de acceso a internet.
GUSANO DE INTERNET: se propagaba con gran facilidad en máquinas UNIX.

2. Bombas Lógicas (Logic Bombs). este código dañino se activa al producirse un hecho predeterminado, como por ejemplo una fecha, un número de encendidos del sistema, determinada secuencia de teclas, etc.

3. Puertas Trampa. Son puntos de entrada secretos en un programa, creados para facilitar la depuración sin pasar por el segmento de autenticación pueden ser instalados en el código fuente para suministrar accesos ilegales. Un ejemplo son los Easter Egg [9].

4. Caballos de Troya (Trojan Horses). Son códigos dañinos anexados en programas de uso autorizado, que al ser ejecutados permiten que dicho código nocivo tome el control del sistema.

5. Bacteria. No realiza daños a sí mismo, su propósito es replicarse a sí misma, puede hacer sólo dos copias de sí misma. Su efecto nocivo es el de consumir todo el especio en memoria y en disco negando el acceso de los usuarios a los recursos.

6. Virus: Son programas, rutinas o instrucciones desarrolladas para provocar la destrucción o alteración de información importante en un sistema. Tanto el código ejecutable, como el código no ejecutable son susceptibles de ser infectados, pero sólo adquiere capacidad de autoreproducirse cuando infecta código ejecutable.

Características de los Virus:

- Se crean y programan intencionalmente.
- Se introducen en equipos de cómputo en diferentes formas
- Deben ser activados para que realicen su función nociva, debido a que dependen de un archivo ejecutable que los carga en memoria.
- Se camuflen en programas o archivos de apariencia normal.
- Algunos virus tienen la capacidad auto-encriptarse para evitar ser detectados por los Antivirus.

[9] Egg Heaven 2000. Available from Internet: <http://www.eggheaven2000.com

Cronología de los Virus:
Cuadro 1. Cronología acerca de los orígenes de los virus.

1939-1949:	John Louis Von Neumann, colaborador en la construcción de las célebres computadoras ENIAC y UNIVAC, demuestra la posibilidad de crear pequeños programas con capacidad para tomar a su vez el control de otros programas. Nadie sospechó en un principio las consecuencias....
1959:	En los laboratorios AT&T Bell, se inventa el juego "Guerra Nuclear" (Core Wars). Consistía en una batalla entre los códigos de dos programadores, en la que cada jugador desarrollaba un programa cuya misión era la de acaparar la máxima memoria posible mediante la reproducción de sí mismo.
1970:	El Creeper es difundido por la red ARPANET. El virus mostraba el mensaje "SOY CREEPER...ATRAPAME SI PUEDES!". Ese mismo año es creado su antídoto: el antivirus Reaper cuya misión era buscar y destruir al Creeper.
1980:	La red ARPANET (fue la red precursora de Internet) es infectada por un "gusano" y queda 72 horas fuera de servicio. La red, que utilizaba UNIX como sistema operativo se vio afectada en 6.000 servidores.
1983:	El juego Core Wars, salió a la luz pública. Ese mismo año aparece el termino virus tal como lo entendemos hoy.
1986:	Un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. VIRDEM podía infectar cualquier archivo con extensión .COM. Aparecen, pues, en escena los primeros virus capaces de infectar archivos .EXE y .COM.
1987:	Se da el primer caso de contagio masivo de computadoras a través del MacMag Virus, sobre computadoras Macintosh. El virus contaminó el disco maestro del nuevo software Aldus Freehand que fue enviado a la empresa fabricante que comercializó su producto infectado por el virus.
1988:	El virus Brain creado por los hermanos Basit y Alvi Amjad de Pakistán aparece en Estados Unidos. El primer virus destructor y dañino plenamente identificado que infecta muchos PCs fue creado en 1986 en la ciudad de Lahore, Pakistán, y se le conoce con el nombre de BRAIN. Este virus infectaba el sector de arranque de los disquetes. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Wordstar, etc por sumas bajísimas. Los turistas que visitaban Pakistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20,000 PCs. Los códigos del virus Brain fueron alterados en los EE.UU., por otros programadores, dando origen a muchas versiones de ese virus, cada una de ellas peor que la precedente.
1989:	Año de efervescencia viral. Virus como el "Fu manchú", "Jerusalem", "Datacrime", "Stoned", ponen en alerta a usuarios y empresas del peligro real y el coste económico que conlleva la infección de virus.
1991:	Aparición del primer virus polimórfico. Symantec comercializa "Norton Antivirus". Los macro virus aparecen en escena, familia de virus con capacidad para infectar documentos y replicarse infectando otros documentos sin ser archivos ejecutables. Alerta mundial frente al virus "Michelangelo".
1998:	El año del Back Orifice, primer virus Troyano diseñado para la administración remota de equipos.
1999:	Aparecen los virus con la más terrible capacidad de difusión: Los virus adjuntos a mensajes de correo (Melissa, Magister, Chernobyl, Sircam, BubbleBoy...)
2000:	El virus I Love you fue detectado el Jueves 4 de mayo de 2000 cuando infecto a miles de ordenadores en todo el mundo. Este código ha sido considerado como uno de los más rápidos de todos los tiempos en propagarse e infectar ordenadores.
2001:	El virus Sircam (2001): Llegaba oculto dentro del contenido de un mensaje de correo electrónico, fue considerado muy peligroso por el gran número de infecciones que produjo. Combinaba caracterís ticas de troyano y gusano de Internet y también fue conocido por la frase que encabeza el mensaje: ¿Hola como estas?
2002:	El virus Klez , el más persistente, en su momento causó estragos por su capacidad para aprovecharse de vulnerabilidades en aplicaciones como los navegadores de Internet o los clientes de correo electrónico, con el fin de autoejecutarse simplemente con la vista previa del mensaje de email en el que llegan.
2003:	Blaster apareció en septiembre del 2003, atacaba básicamente el sitio de Microsoft. Este gusano se propagó rápidamente a través de computadoras con Windows 2000 y XP.
2004:	El gusano MyDoom.A, se propaga a través del correo electrónico en un mensaje con características variables y a través del programa de ficheros compartidos (P2P) KaZaA
2005:	El virus informático más molesto del 2005 fue el Elitper.D, por impedir él sólo la ejecución de hasta noventa aplicaciones comunes, como Word, Excel o Winzip. El titulo más moderno los ostenta ComWar.A, el primer virus para teléfonos móviles capaz de enviarse a sí mismo en mensajes MMS, de la misma manera en que lo hacen los del correo electrónico. El troyano Bancos.NL, fue el más observador, ya que espía al usuario a la espera de que éste entre en la Web de entidades bancarias para robarles los datos.
2006:	Para el 2006, se va a ver una proliferación de virus cada vez más compleja y más oculta con un objetivo lucrativo, como los troyanos, keyloggers, phishing y pharming. Las amenazas saltarán a plataformas nuevas como las de 64 bits o los dispositivos móviles.

Fuente: Boletín No.19 Por Anellie Guillen. www.gcpglobal.com

Medios de Infiltración de los virus. Los medios comúnmente utilizados por los virus para su infiltración son:

Unidades externas de Almacenamiento:

- Unidades de discos extraíbles.
- Disquetes.
- CD Rom.
- Otros formatos extraíbles.

Conexiones externa de datos:

La información que accede al ordenador a través de una conexión de datos puede servir de vía de acceso para los virus, por lo tanto el hecho de conectar equipos a redes informáticas incrementa las posibilidades de resultar infectado por virus informáticos. Es así como Internet ha colaborado en forma masiva con la difusión de virus informáticos, ya que la enorme cantidad de usuarios conectados trasvasando información, descargando archivos, recibiendo y enviando correo han convertido la red en el medio ideal para la difusión masiva de estos dañinos programas.

Dentro de Internet se diferencian tres principales vías de entrada:

Descarga de archivos. Descargar o compartir todo tipo de archivos, sonido, imágenes, utilidades y programas.

Correo electrónico. Archivos adjuntos, Mensajes enviados por equipos infectados por virus que se auto envían a toda o parte de la libreta de direcciones o a cualquier dirección de correo que encuentren en la caché del navegador sin intervención del usuario. Ciertos virus de nueva generación no necesitan adjuntar archivo, son capaces de infectar simplemente abriendo el mensaje de correo, o ni tan siquiera eso si se tiene activada la vista previa de Outlook Express, ya que aprovechan un bug de Microsoft.

Sitios WEB. Si nuestro navegador está configurado para aceptar la ejecución de controles Active X y aplicaciones de Java estamos autorizando a una aplicación ejecutar algo que... suponemos que es benigno. La suposición es la madre del error, decían en la antigüedad.

Aunque los documentos en html por sí solos no tienen capacidad de infección, es posible quedar infectados con sólo visitar una página en Internet. Los virus se apoyan en técnicas como la llamada ingeniería social cuando ofrecen algo atractivo, un señuelo adecuado al gusto o moda del momento, una oferta que no se pueda rechazar, por ejemplo, las páginas de contenido sexual son las más visitadas en la red. Es famoso el virus cuyo señuelo consistía en el ofrecimiento de una imagen de la tenista Anna KourniKova desnuda. El oportunismo es también utilizado dentro de la ingeniería social para insertar virus, sobre todo si el correo

proviene de una persona conocida. Recordemos los virus que aluden a fechas en las que es normal recibir correos de felicitación, como los que aluden fechas especiales como ”Feliz Navidad”. Otro señuelo de fuerte atractivo es la curiosidad y el morbo, en ocasiones aderezado con temas de actualidad como los hechos ocurridos a las torres gemelas, o la guerra entre Estados Unidos contra Irak. Una reciente técnica de ingeniería social aparece en ocasiones bajo la fachada de un boletín oficial de alguna organización bastante conocida, advierte del riesgo de un nuevo virus muy peligroso y dañino que puede destruir la BIOS, infectar ejecutables entre otros. Aconseja además, descargar un parche de seguridad desde un link que conduce en realidad a un sitio que contiene el troyano. La dirección “http://www.microsoft.com@”, advierte de las direcciones web que incluyen el símbolo de la arroba, técnica adoptada para encubrir la verdadera localización y remitir a un site gemelo creado para tal efecto. No se puede confiar de las ventanas que surgen en ciertas páginas web, en las cuales se debe elegir cierta opción, debido a que algunos virus scripts para html pueden superponer dicha ventana a la del navegador, en la que se pide autorización para ejecutar el código, en este caso infectado. Aceptando la ventana falsa estamos autorizando la ejecución del programa maligno.

Fases de Infección de los Virus:

- **Fase de Propagación o Reproducción:** el virus hace copias de sí mismo en otros programas. Su funcionamiento es igual al de cualquier algoritmo de copia.

- **Fase de activación o ataque:** el virus se activa para realizar la acción nociva para la cual fue diseñado. Al introducirse el virus, procederá a ocultarse para infectar archivos o esperar el momento de ejecutar su código de ataque, y con él sus rutinas dañinas. Este se puede alojar en el disco duro, bajo la apariencia de un archivo normal, sector de arranque, memoria principal, documentos con macros, entre otros.

- **Fase de ejecución:** se ejecuta la función que puede ser inocua (mensaje en pantalla) o muy dañina (formatear un disco).

- **Fase de Defensa:** tiene como objetivo la protección del virus, el retardo en su detección, evitando todo aquello que provoque la remoción del virus. Es el módulo inteligente del virus.

7. Spam: no es un código dañino, pero si bastante molesto. Se trata de un programa que ejecuta una orden repetidas veces. Normalmente en el correo electrónico. Así un mensaje puede ser enviado varios cientos de veces a una misma dirección. En cualquier caso existen programas anti spam, ya que los spam son empleados normalmente por empresas de publicidad directa.

8. Negación de Servicio (DoS): en este tipo de ataque el pirata informático mediante maniobras técnicas busca negar completamente un servicio requerido ya sea por un usuario, red sistema o recurso legítimo. Las consecuencias en costos económicos son muy altas y corresponden al lapso de tiempo de indisponibilidad que el sistema haya estado, junto con todo el esfuerzo necesario realizado para identificar y corregir este ataque.

Ejemplos de estos tipos de ataques tenemos los efectuados en el mes de febrero del 2000 a algunos sitios web como yahoo.com, Buy.com, CNN.com los cuales fueron dejados sin funcionamiento por dos días. También en el año de 1999 el F.B.I y otros organismos del gobierno de los E.E.U.U, recibieron ataques como venganza por sus investigaciones en contra de piratas informáticos.

Tipos de Ataques de Negación de Servicio (DoS). Existen en el mercado muchas herramientas disponibles para lanzar ataques de negación de servicio, por lo tanto es de gran utilidad identificar los tipos de ataques que pueden suceder con el objeto de detectarlos y tomar las medidas necesarias para contrarrestarlos:

1. Consumo de Ancho de Banda. La idea de este tipo de ataque es consumir todo el ancho de banda disponible en una red. Este puede suceder sobre una red local, pero es más frecuente que el ataque consuma recursos remotamente. Este tipo de ataque presenta dos estilos, el primero consiste en inundar la conexión de red atacada debido a que el atacante posee más ancho de banda disponible, por ejemplo que tenga un enlace T1 con 1,544 Mbps contra alguien que tenga un enlace de red de 128 Kbps.

El segundo estilo de ataque consiste en amplificar su ataque de negación de servicio, uniendo varios sitios para inundar la conexión de red objetivo de ataque. Esta situación permite que alguien que disponga de un enlace de red más pequeño por ejemplo de 56 Kbps pueda llegar a saturar completamente a una red con acceso T3 de 45 Mbps, para lograrlo es necesario que el atacante reúna los sistemas amplificando el ataque DoS para que envíen el tráfico a la red objetivo de ataque para así inundarla y dejarla fuera de funcionamiento.

2. Inanición de recursos: es un tipo de ataque DoS enfocado más hacia el consumo de recursos del sistema que a los recursos de red. Los efectos de este ataque se traducen en saturación de memoria, CPU, sistemas de archivos y otros procesos propios del sistema. Se manifiestan externamente mediante fallos generales del sistema, copamientos del sistema de archivos o que los procesos se queden colgados.

3. Defectos de programación (programming flaws). Son ataques que aprovechan los fallos de una aplicación, sistemas operativos que dejan sin respuesta los sistemas ante condiciones de excepción. Ejemplos de estos ataques tenemos DoS f00f del Pentium que hace que un proceso en modo usuario cuelgue

a cualquier sistema operativo con sólo ejecutar la instrucción 0xf00fc7c8 no válida.

4. Ataques de Enrutamiento y DNS. Consiste en la manipulación de las tablas de enrutamiento o distribución con el fin de denegar el servicio a sistemas o redes legítimos. Resulta que los protocolos de enrutamiento tales como Routing Information Protocol (RIP) v1 y Border Gateway Protocol (BGP) v4 no tienen o poseen una autenticación muy sencilla, que rara vez es utilizada o activada cuando se instalan dispositivos de enrutamiento, por lo tanto se facilita a los atacantes para que cambien las rutas legítimas y frecuentemente falsifican su dirección IP de origen creando otro tipo de ataque de negación de servicio.

Existe otro tipo de ataque de este tipo y se efectúa sobre servidores de nombres de dominio (DNS). Tratan de convencer al servidor DNS víctima para que guarde direcciones falsas en la caché. Provocando que el servidor DNS al efectuar una búsqueda, redireccione al sitio del atacante.

Formas de Ataque a la Seguridad Informática.

Un ataque puede presentarse en diversas formas clasificadas en cuatro categorías tales como (Figura 5):

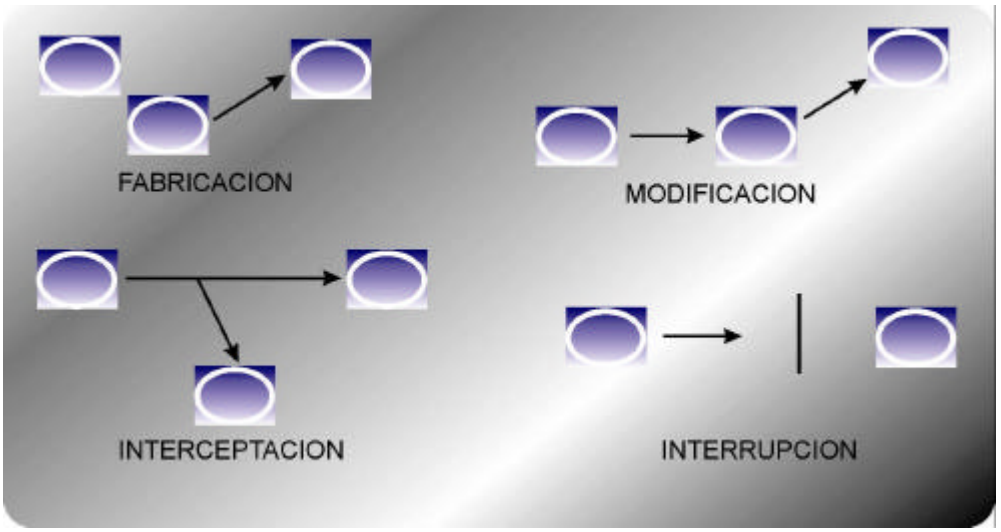
a. Fabricación. Se refiere a aquella maniobra técnica o de engaño humana que es elaborada o diseñada para actuar contra un objetivo definido, por ejemplo los virus.

b. Modificación. este ataque persigue alterar o cambiar ya sea información o sistemas sensibles para la organización. Por ejemplo la alteración de un servidor que contiene las notas de los estudiantes de una Universidad.

c. Interceptación. Relacionados con aquellas estrategias técnicas o de engaño humano que permiten enterarse sin que nadie lo note de información pertinente exclusivamente a la organización. Ejemplo de esto pudiera ser un pinchazo electrónico o la utilización de un "sniffer" en la red de la empresa objetivo de ataque.

d. Interrupción. Este tipo de amenaza persigue cortar la transmisión de información, como sucede cuando un servidor deja de funcionar debido a un ataque de negación de servicio.

Figura 5. Formas de Ataque a la Seguridad Informática



Fuente: Seguridad Informática, Especialización en Redes y Telecomunicaciones UIS.

Métodos de Ataque. Las anteriores formas de ataque han originado diversos métodos que los atacantes usan para intentar penetrar las organizaciones como por ejemplo: las contraseñas, escuchas en las líneas, instalar cámaras ocultas o hasta revisar las cestas de la basura para conseguir la información objetivo. El proceso de ataque generalmente no es instantáneo, sino que generalmente es progresivo, es decir se van colocando más retos, penetrando cada vez más y elevando sus privilegios dentro de la organización. Dentro de sus objetivos importantes pueden estar los sistemas de archivos, ya que pueden ejecutar programas de administración y obtener permisos, también son conocedores de los archivos de registro porque les permite borrar los rastros de su intrusión, y así entrar las veces que deseen sin que nadie se entere. Lo piratas informáticos pueden crear también las llamadas puertas traseras en el sistema con el objetivo de poder acceder más tarde en caso de que su forma de acceder habitualmente sea descubierta. Dentro de los métodos más comunes y efectivos de atacar tenemos:

1. Invasiones del puesto. Consiste en espiar a las personas aprovechando que han dejado su puesto de trabajo libre durante el cual se instala, extrae, engaña o revisa información sensible. Ejemplo de este ataque lo relata el analista de seguridad Bill Hancock, en un artículo de abril de 1996 llamado “Can you Social Engineer Into Your Network” aparecido en la revista Network Security (Oxford, UK). Dice que un día entró a una oficina sucursal de la compañía, dijo a los empleados que pertenecía a la oficina principal, y que necesitaba un sitio donde pudiera trabajar antes de tomar el avión, sorpresa enorme se llevó debido a que le

ofrecieron una oficina con una conexión activa a la red de la empresa. En otra ocasión creó una tarjeta falsa con el logotipo de la compañía y un trozo de cinta magnética para simular la banda magnética. A pesar de que esta estrategia no le sirvió totalmente, pudo acceder a áreas reservadas de la compañía esperando que alguien autorizado entrara, sosteniendo la puerta tras él. Una vez adentro logró el puesto de las copias de seguridad y lo utilizó para romper el 50 por ciento de las contraseñas.

2. Ataques Telefónicos. Este tipo de ataques es perpetrado por personas que sacan ventaja del sistema de telecomunicaciones, efectuando llamadas telefónicas de larga distancia gratis, pueden también escuchar conversaciones privadas, acceder otros sistemas a través del sistema violado, acceder a sistemas internos. Por lo tanto son personas expertas en conmutadores telefónicos, redes, equipos de redes, sistemas PBX, armarios telefónicos, cuartos de telecomunicaciones, poseen manuales de fabricantes de equipos de telecomunicaciones, dentro de sus maniobras, está el hacer una llamada a una empresa, transferir la llamada a un operador, para luego simular que es un empleado importante de la empresa y que necesita una llamada al exterior, la llamada es ahora de la compañía que es la que paga y lo peor es que puede aparecer como responsable de otros ilícitos. Otra técnica empleada es la guerra telefónica (wardialing), esta consiste en utilizar un programa de automarcado telefónico, con el fin de encontrar los números telefónicos de computadoras conectadas por modem, marca sucesivamente números telefónicos, cuando encuentra un modem el número es guardado en un registro, mientras el programa sigue buscando. Luego el atacante toma los números telefónicos y marca a cada uno de los teléfonos guardados intentando penetrar el sistema. En cuanto a herramientas con las que se puede desarrollar estos tipos de ataques están ToneLoc y THC- Scan, son totalmente gratuitos y pueden bajarse de internet, también existe una comercial llamada PhoneSweep.

3. Pirateado de cuentas y contraseñas. Obtener el nombre y las contraseñas de las cuentas de los usuarios es una de las primeras prioridades de los atacantes, porque de lograrlo el siguiente paso sería mejorar los privilegios, además los nombres de usuarios son fáciles de adquirir, pues en muchas organizaciones los usuarios internos tienen fácil acceso a listas de nombres de usuarios, además los sistemas de correo electrónico en una empresa pueden suministrar este tipo de listas, por lo tanto se debe asegurar que estas listas no sean legibles. Si el atacante llega a obtener un nombre de cuenta de usuario, procedería a romper la contraseña, para romperla se apoyan en contraseñas comunes y fáciles de adivinar que muchos usuarios utilizan como el nombre de sus hijos, mascotas, fechas de nacimiento entre otras. Muchas personas utilizan la misma contraseña que en otros sistemas como los cajeros electrónicos, un atacante podría robar la contraseña observando a larga distancia con unos binóculos, también pudiera intentar romper la contraseña mediante un ataque de fuerza bruta, esto consiste en un programa que intenta sucesivamente miles de contraseñas diferentes hasta que logra el acceso. Este método resultaría ineficiente si el inicio de sesión limita

el número de intentos, como en el caso de Windows NT que limita el número de intentos a tres. Un ataque de diccionario, es muy similar al anterior sólo que utiliza un diccionario completo con contraseñas comunes en varios idiomas. Otro método para romper las contraseñas consiste en instalar programas de captura o lector de teclas de teclado siempre y cuando se tenga acceso a la estación de trabajo.

Estos programas son llamados en inglés keyloggers. El autor de este proyecto en una de las materias cursadas de la maestría hizo la demostración del funcionamiento de una de estas herramientas, la utilizada fué KK2000.

4. Pirateado de sistemas de confianza. Los atacantes adoran las relaciones de confianza, ya que un programa de una computadora puede acceder a información almacenada en otra computadora, permitiéndoles acceder a otros sistemas y más si dichas relaciones son transitivas[10].

5. Escuchas electrónicas y rastreadores de conexiones (Sniffing). Se refiere a un dispositivo o software que instala el atacante en un punto ya sea externo o interno de una organización con el objeto de capturar, almacenar paquetes para posteriormente extractar la información de interés, que son habitualmente los inicios de sesión, esta técnica de escucha es difícil de detectar, estos rastreadores generalmente se conocen con el nombre de sniffers, y uno de los más famosos es el "snort"[11].

6. Otras Areas Vulnerables. Los piratas informáticos hacen uso de una variedad de herramientas y técnicas para atacar. Usualmente se aprovechan de falencias conocidas, dentro de estas tenemos:

a. Archivos y directorios. Existen sistemas operativos con debilidades en sus sistemas de archivos que pueden permitir arrancar equipos con DOS para acceder a archivos de cualquier directorio, por ejemplo en Windows NT uno de sus sistemas de archivos: el FAT permite arrancar una computadora desde DOS permitiendo acceder a cualquier archivo de un directorio, estas debilidades son comúnmente llamadas agujeros de seguridad.

b. Usuarios Móviles y Remotos. El hecho de permitir inicio de sesión a un usuario móvil remoto nos puede ocasionar serios inconvenientes de seguridad, como por ejemplo:

- Alguien puede ver el inicio de sesión del usuario remoto de la compañía, ya sea directamente o utilizando dispositivos de vigilancia cercanos.

[10] Relación Transitiva. Una relación de confianza es transitiva si un sistema X mantiene su relación de confianza con un sistema Y, y este sistema hace lo mismo con el sistema Z, y se puede extender la relación de confianza de X a Z a través de Y.
[11] Disponible gratuitamente en http://www.snort.org/.

- El usuario remoto realiza los inicios de sesión sobre líneas públicas, que pueden no tener la seguridad adecuada, permitiendo el espionaje de piratas informáticos que tengan en la mira nuestra compañía.

- Un equipo portátil puede ser fácilmente objeto de robo. La información valiosa de la organización queda a merced del ladrón como: contraseñas almacenadas en el disco, nombre de las cuentas de usuario listadas en las direcciones de correo electrónico, información confidencial de la compañía entre otras.

c. Puertas traseras. Conocidas en inglés con el nombre de backdoors. Son generadas por los piratas informáticos al abrir puertos utilizando características tanto de las redes, como de los sistemas operativos, que les permiten ejecutar funciones remotas sobre equipos, blanco de ataque. También los programadores habitualmente dejan en sus programas puertas de escape, con el fin de saltarse procesos que ahorran pasos de verificación y control, útiles en el proceso de creación de programas, pero no se percatan u olvidan muchas veces cerrarlos, provocando serios problemas cuando al hallarlos los piratas informáticos, logran aumentar los privilegios hasta acceder a una organización. (Figura 6).

Figura 6. Agujeros de Seguridad.

Fuente: Autor del proyecto.

La siguiente secuencia permite ilustrar lo que es una puerta trasera: para esto se utiliza una herramienta llamada la navaja Suiza TCP/IP, comercialmente conocida con el nombre de NETCAT (véase http://www.10pht.com/netcat), esta se configura para detectar un determinado puerto y luego enviar un ejecutable (shell-intérprete de comandos de Windows NT) cuando exista conexión a ese puerto así:

1. Paso: El hacker logra acceso al equipo objetivo de ataque (c:\) e introduce la herramienta netcat, la configura mediante los siguientes comandos:

```
C:\ temp/nc11nt>nc-L –d-e cmd.exe –p 8080
```

Explicación: Estos le proporcionan una shell remota de comandos a cualquier intruso que se conecte al puerto 8080.

-L: hace que la escucha continúe a través de múltiples interrupciones de conexión.
-d: ejecuta netcat en modo de escucha sigilosa. Sin consola interactiva.
-e: especifica el programa a ejecutar cmd.exe el intérprete de comandos de NT.
-p: puerto donde se escuchará.

2. Paso: El Hacker usa NETCAT remotamente para conectarse con el puerto 8080 que está a la escucha, sabiendo que el equipo blanco de ataque (D:\) tiene la IP 192.160.204.45. Además para recibir una shell de comandos remota**.**

```
D:\ nc 192.160.204.45  8080
Microsoft ® Windows NT ™
Copyright 1995 2004 Microsoft Corp.
```

3. Paso: El hacker logra acceder remotamente al equipo con IP 192.160.204.45

```
C:\TEMP/NC11NT>
C:\TEMP/NC11NT>ipconfig
Windows NT IP Configuration
Ethernet adapter FEM5561
IP Address ..............: 192.160.204.45
Subnet Mask.............: 255.255.255.0
Default Gateway.......:
C:\TEMP/NC11NT>exit
D:\
```

d. Exploración de Puertos: Uno de los pasos que realiza un atacante informático para determinar si los sistemas individuales están activos, es llevar a cabo un barrido ping automatizados por ejemplo en un rango de direcciones IP y bloques de red. La instrucción Ping se utiliza habitualmente para enviar paquetes ICMP ECHO (Tipo 8) al sistema objetivo de ataque, si el sistema responde un ICMP ECHO_REPLY (Tipo 0) indicará que el sistema destino está activo. Por lo tanto una exploración de puertos es el proceso de conexión a puertos (UDP y TCP) del sistema destino que constituyen nuestro objetivo para determinar qué servicios están activos o si se encuentran un estado de escucha (LISTENING).

Los objetivos de este ataque denominado exploración de puertos son los siguientes:

→ La identificación de servicios UDP y TCP que se están ejecutando en el sistema objeto de ataque.

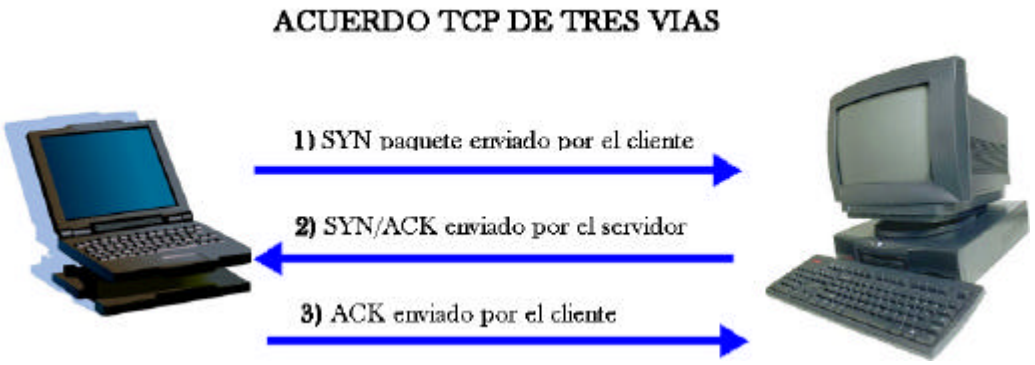
→ La identificación del sistema operativo.

→ La identificación de las versiones o aplicaciones específicas de un determinado servicio.

- Tipos de Exploración: Existe una herramienta desarrollada por Fyodor llamada Nmap, en esta se han desarrollado varios tipos de exploración de puertos dentro de las cuales destacamos:

1. Exploración de conexión TCP. Esta busca conectar con el puerto objeto de ataque e intentar un acuerdo o conexión de tres vías (SYN, SYN/ACK Y ACK). Tiene como gran desventaja que es fácilmente detectable por el sistema atacado. (Figura 7).

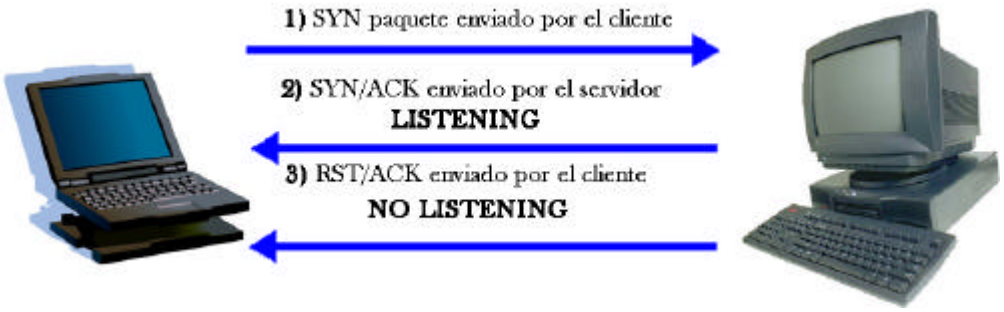
Figura 7. Exploración de Conexión TCP Completa



Fuente: Autor del Proyecto

2. Exploración TCP SYN. Este ataque se caracteriza porque no se realiza una conexión TCP completa, también es conocida como exploración semiabierta. Se envía un paquete SYN al puerto objetivo. Si retorna un SYN/ACK del puerto explorado, se puede deducir que está a la escucha. Si por el contrario, se recibe un RST/ACK esto indicará que el puerto no está a la escucha. Luego el sistema que está llevando a cabo la exploración de puertos enviará un RST/ACK para que no establezca una conexión completa, siendo una técnica más cautelosa y difícil de detectar. (Figura 8).

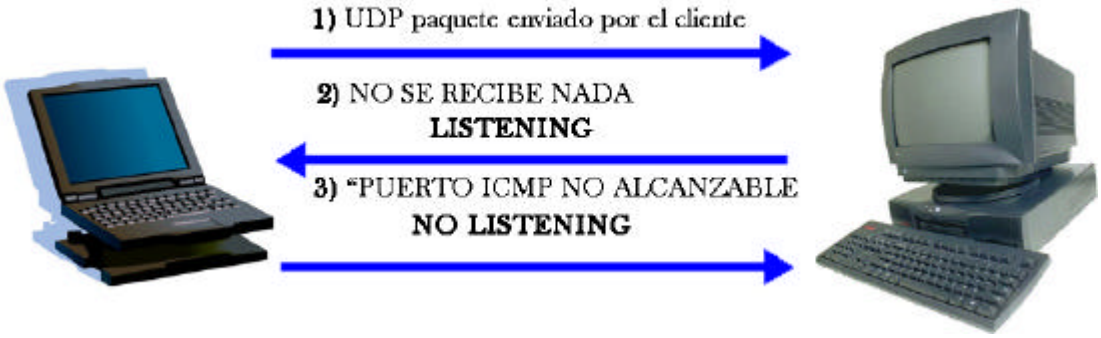
Figura 8. Exploración TCP SYN



Fuente: Autor del Proyecto

3. Exploración UDP. En esta envía un paquete UDP al puerto atacado. Si el puerto responde con un mensaje similar a "puerto ICMP no alcanzable" obviamente el puerto está cerrado. En caso contrario, si recibimos un mensaje diferente al de "puerto ICMP no alcanzable", se puede deducir que el puerto está abierto. Como UDP es conocido como un protocolo sin conexión depende de factores relacionados con tráfico y recursos de red, convirtiendo la exploración UDP en un proceso bastante lento. (Figura 9).

Figura 9. Exploración UDP



Fuente: Autor del Proyecto

e. Amenazas Naturales. Es erróneo pensar que todas las amenazas a la seguridad de una red informática provienen del talento humano, también fallos en la alimentación eléctrica, fallos en los componentes, y otras problemáticas pueden arruinar sistemas y provocar enormes pérdidas económicas. Dentro de las amenazas naturales podemos considerar las siguientes:

- Fallos de hardware pueden ocasionar pérdidas en la disponibilidad de los datos, es por eso que los sistemas redundantes y las copias de seguridad son imprescindibles.

- Las interrupciones en la energía eléctrica pueden ocasionar indisponibilidad de la información. Las fuentes de alimentación para copias de seguridad son indispensables.

- Las inundaciones, el fuego, los temblores de tierra y otros desastres obligan a la necesidad de sistemas de copia de seguridad, centros alternativos de datos y plantas de recuperación ante catástrofes.

2. ANALISIS DE VULNERABILIDADES ENCONTRADAS EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

En el capítulo anterior, se realizó un estudio acerca de las principales amenazas que puede afectar hoy en día a cualquier organización, con el fin de evaluar en este módulo cuáles de estas pueden impactar o afectar a la UIS. Este capítulo tiene como objetivo los siguientes:

- Describir la infraestructura de la red de datos institucional de la UIS e identificar los activos organizativos de la UIS.

- Estudiar y analizar las vulnerabilidades encontradas en la UIS (Evaluar el riesgo).

2. 1 IDENTIFICACIÓN DE LOS ACTIVOS ORGANIZATIVOS.

Se relaciona con la creación de una lista que contiene todos los recursos que precisen protección. Los recursos que deben ser considerados al estimar las amenazas a la seguridad se clasifican en seis grupos:

- Hardware: ordenadores y equipos de telecomunicación.

- Software: programas fuente, programas objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

- Datos: copias de seguridad, registros de auditoría, bases de datos, datos en tránsito sobre medios de comunicación.

- Elemento Humano: usuarios, personas para operar los sistemas.

- Documentación: sobre programas, hardware, sistemas, procedimientos administrativos.

- Accesorios: papel, formularios, cintas, información grabada.

Por lo tanto en los ítems siguientes se muestra la identificación de activos correspondientes a la UIS.

2.1.1 Infraestructura de la red de datos institucional de la UIS. Los equipos en los edificios y el centro de cableado principal se instalaron a finales del año 2000 y la fibra óptica data del año 1995. En el 2000 se renovaron los switches de la red utilizando la misma estructura de cableado. Actualmente deben haber unos 3000 puntos de red en la Universidad.

Topología. El equipo principal es un Switch marca Avaya modelo Cajun P880 tipo Enterprise. La topología de la red es en estrella, en su parte central se encuentra el Centro de Cableado Principal de la red que aloja el switch principal, que se encuentra ubicado en el edificio de la planta telefónica (cerca a la biblioteca central), que está más o menos en la mitad del campus para optimizar las distancias de la fibra óptica. A continuación se muestra su estructura modular:

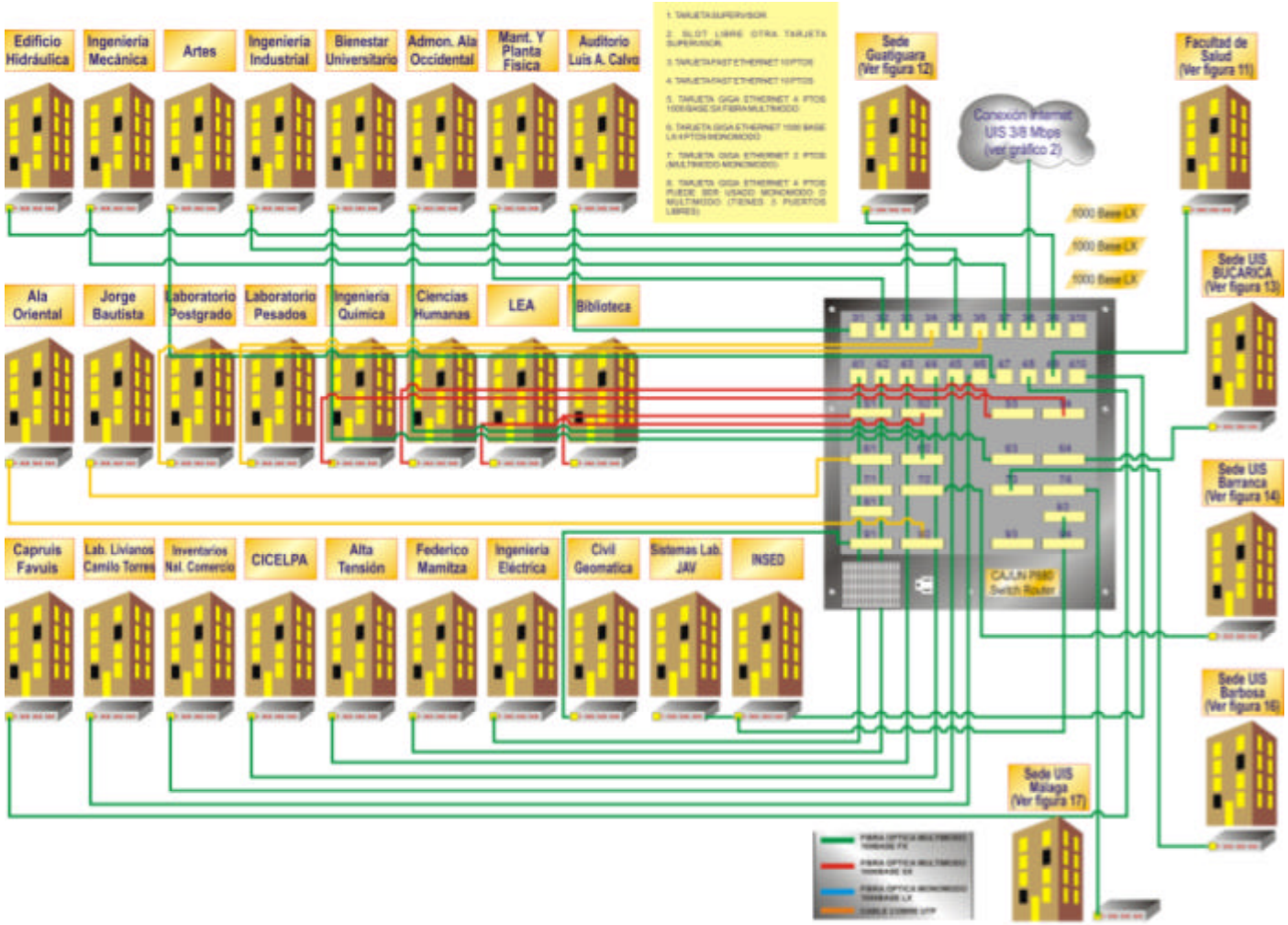
Cuadro 2. Estructura del Switch AVAYA modelo Cajun P880 tipo Enterprise

Tarjeta	Estructura del Switch AVAYA modelo Cajun P880 tipo Enterprise: Velocidad de procesamiento, conmutación y enrutamiento de 55 Gigabits/sg	No De Puertos
1	TARJETA SUPERVISOR	-
2	SLOT LIBRE OTRA TARJETA SUPERVISOR	-
3	TARJETA FAST ETHERNET	10
4	TARJETA FAST ETHERNET	10
5	TARJETA GIGA ETHERNET 1000BASE SX (FIBRA MULTIMODO)	4
6	TARJETA GIGA ETHERNET 1000BASE LX (MONOMODO)	4
7	TARJETA GIGA ETHERNET 1000BASE LX O SX (MULTIMODO-MONOMODO)	4
8	TARJETA GIGA ETHERNET 1000BASE LX O SX (MULTIMODO-MONOMODO)	2
9	TARJETA GIGA -ETHERNET GBIC (PUEDE SER USADO MONOMODO O MULTIMODO) TIENE 3 PUERTOS LIBRES	4
TOTAL		38

Fuente: Autor del Proyecto

Desde este lugar parte el cableado de fibra óptica multimodo a cada uno de los edificios de la universidad: 26 edificios en el campus principal, 5 edificios en la facultad de salud y 6 campus que son Bucarica, Guatiguará, Barrancabermeja, Socorro, Barbosa, Málaga y la Facultad de Salud donde en cada uno existe el centro de cableado que atiende el edificio o la sede, al cual llega la fibra óptica desde el Centro de Cableado Principal. (Ver Figura 10).

Figura 10. Conectividad UIS – Sede Principal



Fuente: Autor del proyecto

Centros de cableado y racks de comunicaciones.

El armario para el cableado sirve como el punto de unión central para el cableado y el equipo de cableado, que se usa para conectar dispositivos en una red de área local (LAN). Es el punto central de una topología en estrella. El armario para el cableado puede ser una habitación o un gabinete diseñado especialmente. Por lo general, el equipo de un armario para el cableado incluye:

Cuadro 3. Dispositivos de un rack de Comunicaciones – UIS

• Paneles de conexión	• Switches
• Hubs de cableado	• Routers
• Puentes	

Fuente: Autor del proyecto.

En cada uno de los edificios del campus principal y demás campus, la fibra óptica se recibe en un centro de cableado ubicado en un cuarto situado en forma tal que todas las tomas de datos de todos los puestos de trabajo de ese edificio, queden a una distancia menor de 100 metros. Esto, con el fin de que todas las tomas de datos cumplan con el parámetro de distancia exigido por la norma de cableado estructurado ANSI/TIA 568A para redes LAN Categoría 5.
El centro de cableado de cada edificio está conformado por un rack estándar de comunicaciones, tipo abierto, de 19" x 7' de aluminio para soportar todos los dispositivos de comunicaciones y de cableado del edificio.

Los dispositivos y elementos que se encuentran en un rack típico de la universidad son:

Un Patch Panel con bandeja para fibra óptica de 16 puertos, con conectores duales tipo ST, para conectorización y soporte de las fibras del cable que viene del Centro de Cableado Principal.

Un Patch Panel de datos con conectores RJ45 Categoría 5, cada uno de los cuales recibe un cable UTP proveniente de una toma de datos en un puesto de trabajo del edificio.

Regletas telefónicas o patch panels telefónicos que reciben el cable UTP de la toma de voz en el puesto de trabajo y la conectan a la red telefónica de la universidad.

La fibra se recibe en cada uno de los edificios en un switch AVAYA P330T de 24 puertos RJ45 10/100 Base TX autosensing, donde se conectan los hubs,

servidores o PCs de ese edificio. El sistema de hubs apilables son Ethernet 10BaseT, conformado por uno (1) o más hubs, hasta un máximo de diez (10). Los hubs utilizados son marca UB-Networks modelo Access/Stax AH1600M, o COMPAQ Netelligent modelo 2016, de 16 puertos, administrabas vía SNMP MIB 11, segmentables y con soporte de BootP/TFTP y XMODEM. El primer hub de la pila dispone de un conector de fibra óptica FOIRL 10BaseFL para conectar la pila a la fibra óptica.

De los centros de cableado de cada edificio, se llega a los puestos de trabajo por medio de un sistema de cableado estructurado certificado como categoría 5 y 5E según las normas ANSI/EIA/TIA 568 (Cable UTP).

La conexión al central puede ser Fast Ethernet (100 Mbps) o GibabitEthernet (1000 Mbps) dependiendo del tamaño y tráfico de la red del edificio como de sus necesidades. Por ejemplo se necesita más velocidad para el edificio de Civil/Sistemas que para el Auditorio Luis A. Calvo.

A continuación se detalla la conectividad de los diferentes edificios y campus de la UIS con el switch principal:

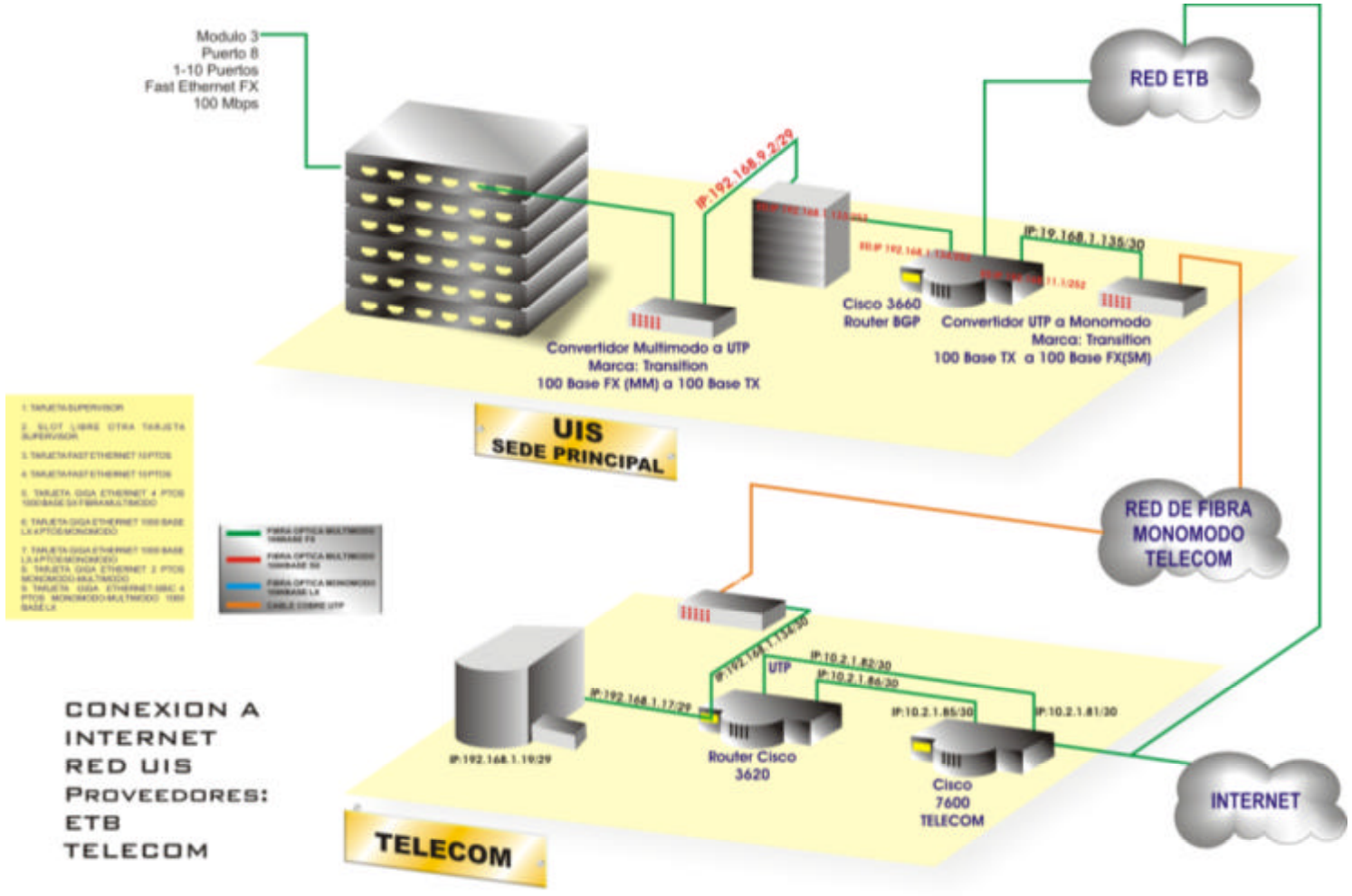
Cuadro 4. Conectividad de la TARJETA 3 FAST ETHERNET Switch Avaya modelo Cajun P880 tipo Enterprise

TARJETA 3	Conectividad de la TARJETA FAST ETHERNET 10 PTOS componente del Switch Avaya modelo Cajun P880 tipo Enterprise	No Tarjeta/ No Puerto
EDIFICIO LUIS A CALVO		3/1
EDIFICIO MANT Y PLANTA FISICA		3/2
CAMPUS GUATIGUARÁ		3/3
EDIFICIO LABORATORIO PESADO		¾
EDIFICIO INGENIERÍA INDUSTRIAL		3/5
EDIFICIO LABORATORIO DE POSTGRADO		3/6
EDIFICIO INGENIERÍA MECANICA		3/7
CONEXIÓN INTERNET UIS		3/8
EDIFICIO HIDRAÚLICA		3/9
LIBRE		3/10
Total		10

Fuente: Autor del proyecto.

La conexión Internet UIS se realiza desde el switch AVAYA P333T con tecnología FastEthernet a 100 Mbps, donde se encuentra la protección de la universidad de ataques externos: el firewall de marca Cisco PIX 515 con una licencia ilimitada de usuarios y conexiones, que es un sistema integrado hardware/software tipo. (Ver Figura 11).

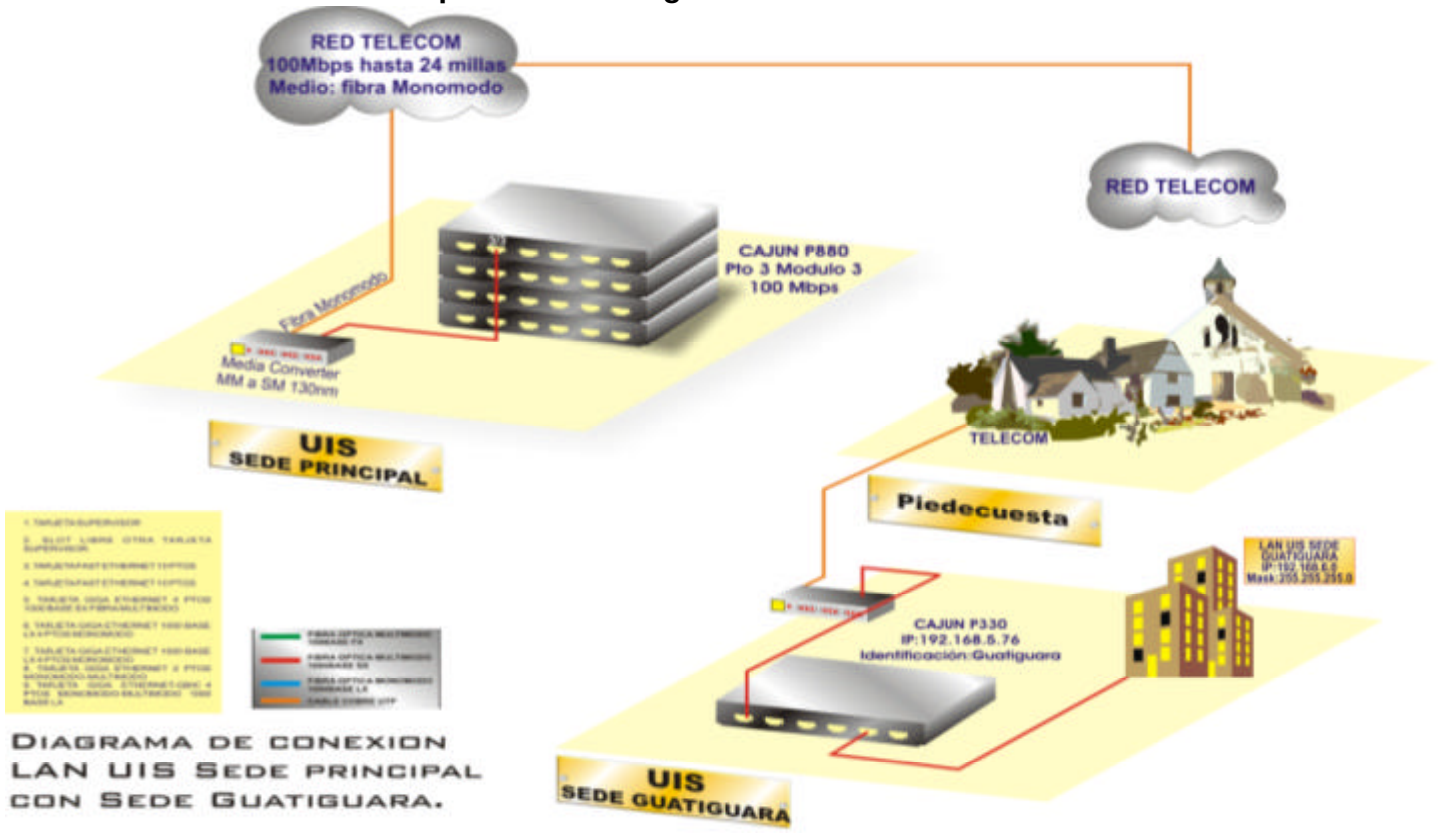
Figura 11. Conexión Internet UIS



Fuente: Autor del Proyecto

El Campus Guatiguará en Piedecuesta es conectado también mediante un switch AVAYA P333T ubicado en el Edificio Administración Ala Oriental y más exactamente en la División de Servicios de Información (D.S.I) de la UIS, mediante un enlace de 128 Kbps contratado con la empresa Telecom. (Ver Figura 12).

Figura 12. Conectividad UIS- Campus Sede Guatiguará



Fuente: Autor del Proyecto

Cuadro 5. Conectividad de la TARJETA 4 FAST ETHERNET componente del Switch Avaya modelo Cajun P880 tipo Enterprise

Tarjeta 4	Conectividad de la TARJETA FAST ETHERNET 10 PTOS componente del Switch Avaya modelo Caj un P880 tipo Enterprise	No Tarjeta/ No Puerto
EDIFICIO INGENIERÍA ELÉCTRICA		4/1
EDIFICIO FEDERICO MAMITZA BAYER		4/2
EDIFICIO ALTA TENSIÓN		4/3
EDIFICO CICELPA		4/4
EDIFICIO ANTIGUA NACIONAL DE COMERCIO		4/5
EDIFICIO LABORATORIOS LIVIANOS (CAMILO TORRES)		4/6
EDIFICIO ARTES		4/7
EDIFICIO CAPRUIS – FAVUIS		4/8
CAMPUS FACULTAD DE SALUD		4/9
EDIFICIO SISTEMAS LABORATORIO JAV		4/10
Total		10

Fuente: Autor del proyecto

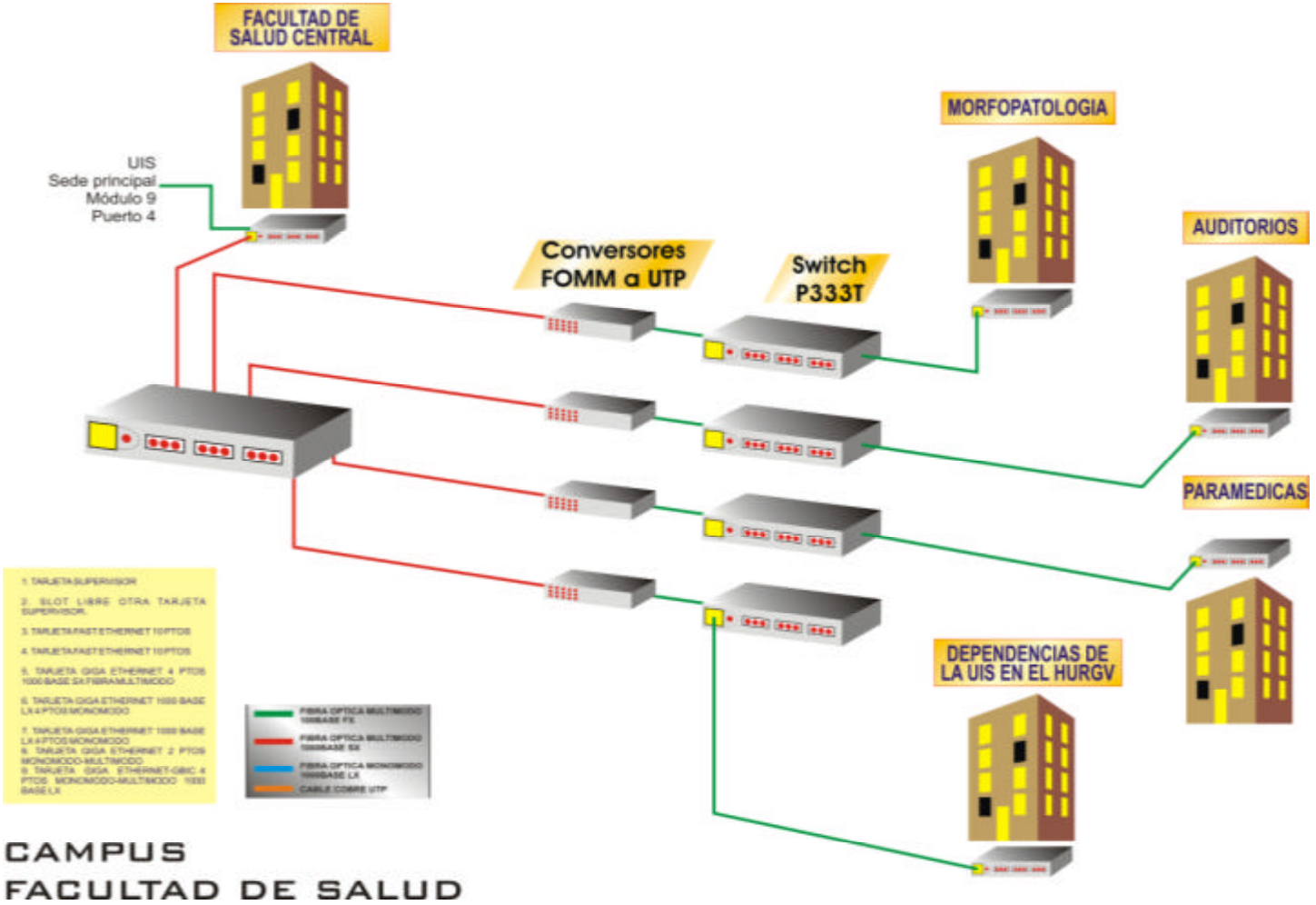
La Facultad de Salud está conectada por medio de fibra óptica multimodo de propiedad de la universidad a 100 Mbps así:

Un switch P333T AVAYA donde se conectan 5 edificios que son:

- Facultad de Salud Central
- Morfopatología
- Auditorios
- Paramédicas
- Dependencias de la UIS en el Hospital Universitario de Santander (Antiguo HURGV).

Cada uno posee un centro de cableado con switches P333T AVAYA donde se conectan los hubs o servidores de los respectivos edificios. (Ver figura 13)

Figura 13. Conectividad UIS- Campus Facultad de Salud



Fuente: Autor del Proyecto

Cuadro 6. Conectividad de la TARJETA 5 GIGA ETHERNET 1000BASE SX FIBRA MULTIMODO componente del Switch Avaya modelo Cajun P880 tipo Enterprise

Tarjeta 5	Conectividad de la TARJETA GIGA ETHERNET 4 PTOS 1000BASE SX FIBRA MULTIMODO componente del Switch Avaya modelo Cajun P880 tipo Enterprise	No Tarjeta/ No Puerto
EDIFICIO BIBLIOTECA		5/1
EDIFICIO LUIS EDUARDO ARIAS (LEA)		5/2
EDIFICIO CIENCIAS HUMANAS		5/3
EDIFICIO INGENIERÍA QUÍMICA		5/4
Total		4

Fuente: Autor del proyecto

Cuadro 7. Conectividad de la TARJETA 6 GIGA ETHERNET 1000BASE LX FIBRA MONOMODO componente del Switch Avaya modelo Cajun P880 tipo Enterprise

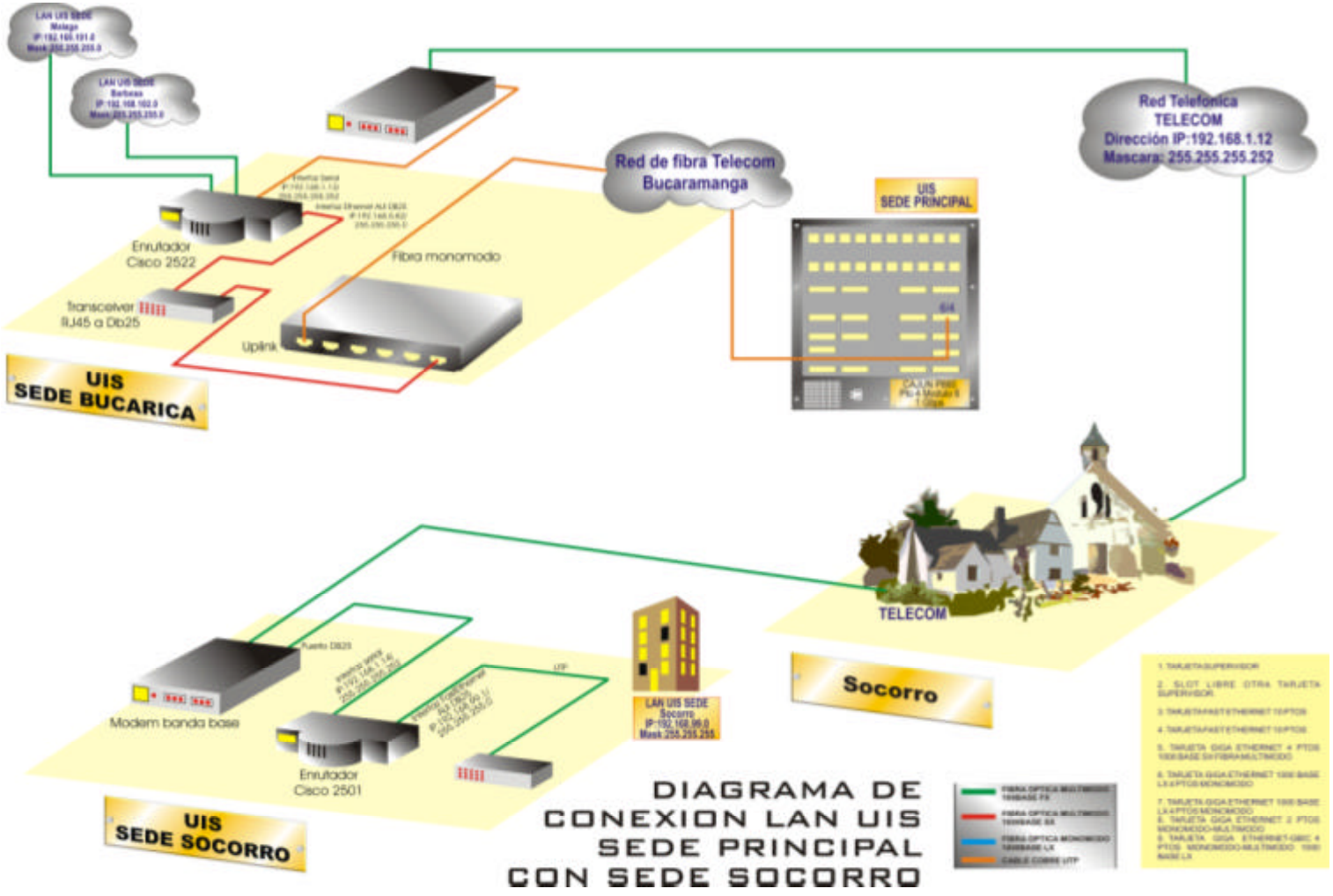
Tarjeta 6	Conectividad de la TARJETA GIGA ETHERNET 1000BASE LX FIBRA MONOMODO componente del Switch Avaya modelo Cajun P880 tipo Enterprise	No Tarjeta/ No Puerto
EDIFICIO JORGE BAUTISTA		6/1
EDIFICIO ADMINISTRACIÓN ALA OCCIDENTAL		6/2
EDIFICO DE BIENESTAR UNIVERSITARIO		6/3
CAMPUS SEDE UIS BUCARICA		6/4
Total		4

Fuente: Autor del proyecto

El campus sede UIS Bucarica está conectado al switch marca AVAYA modelo P880 mediante la tarjeta GigaEthernet -1000BASE LX, para lo cual se emplea fibra óptica monomodo arrendada a la empresa TELEBUCARAMANGA. (Ver Figura 10).

El campus sede Socorro está conectado desde Bucarica a través de un enlace contratado con TELECOM de 256 Kbps.(Ver figura 14).

Figura 14. Conectividad UIS- Campus Socorro



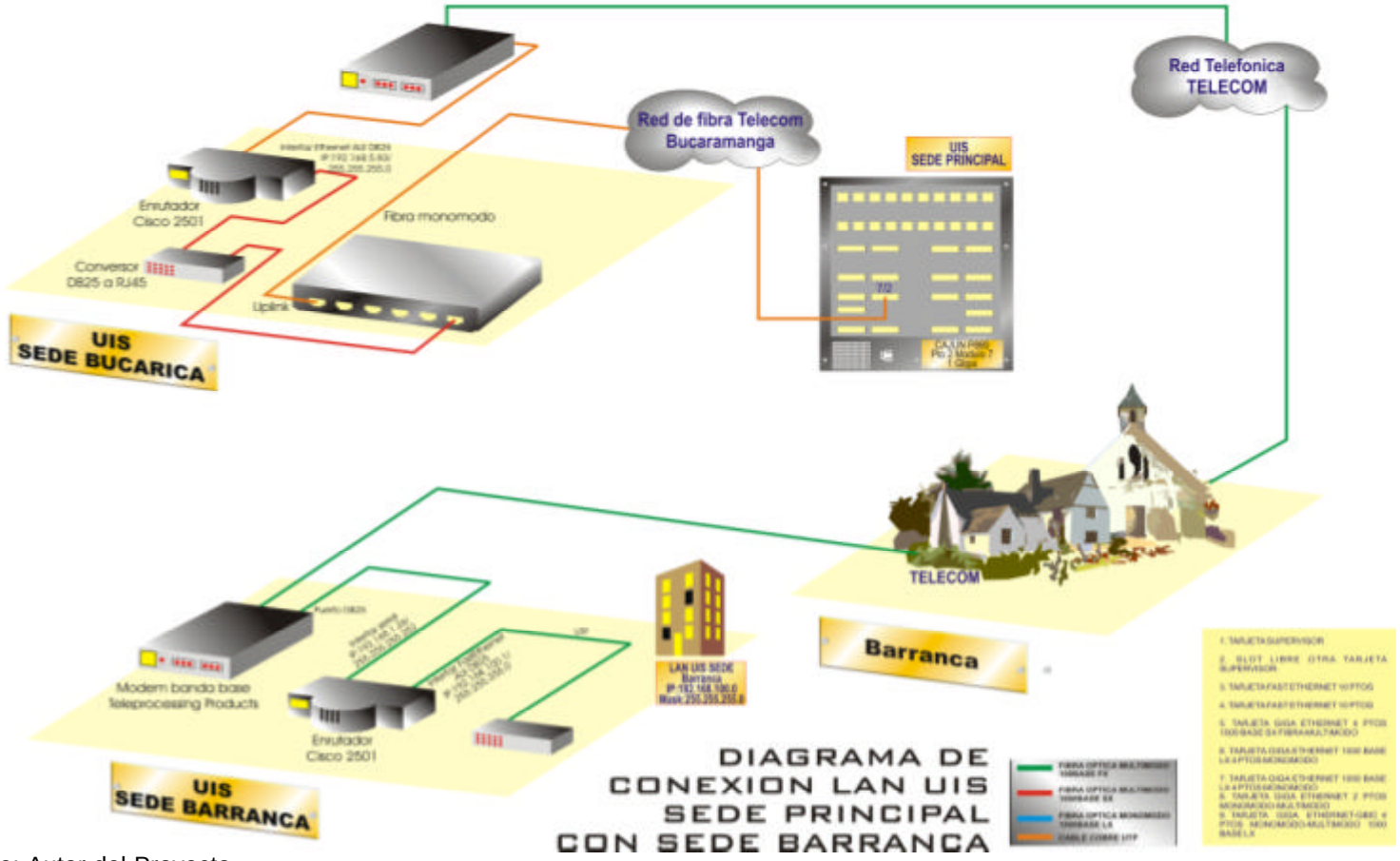
Fuente: Autor del Proyecto

Cuadro 8. Conectividad de la TARJETA 7 GIGA ETHERNET FIBRA MONOMODO componente del Switch Avaya modelo Cajun P880 tipo Enterprise

Tarjeta 7	Conectividad de la TARJETA GIGA ETHERNET FIBRA MONOMODO componente del Switch Avaya modelo Cajun P880 tipo Enterprise	No Tarjeta/ No Puerto
LIBRE		7/1
CAMPUS SEDE UIS- BARRANCABERMEJA		7/2
CAMPUS SEDE UIS- BARBOSA		7/3
CAMPUS SEDE UIS-MÁLAGA		7/4
Total		4

El campus sede Barrancabermeja se conecta al switch principal mediante el Campus Bucarica a través de una tarjeta GigaEthernet 1000BASE LX y de un enlace de fibra óptica monomodo de TELECOM 256 Kbps. (Ver figura 15).

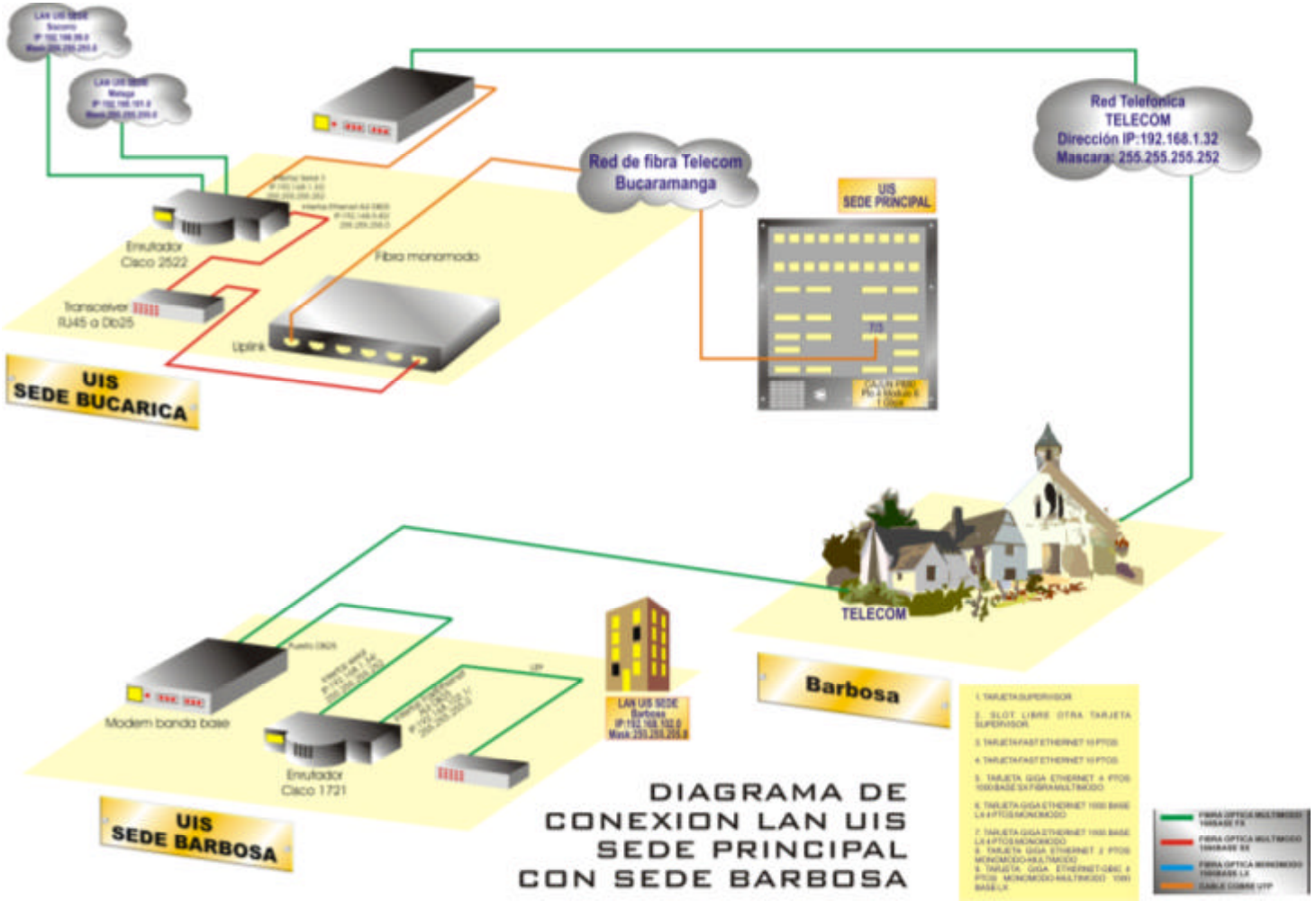
Figura 15. Conectividad UIS- Campus Barranca



Fuente: Autor del Proyecto

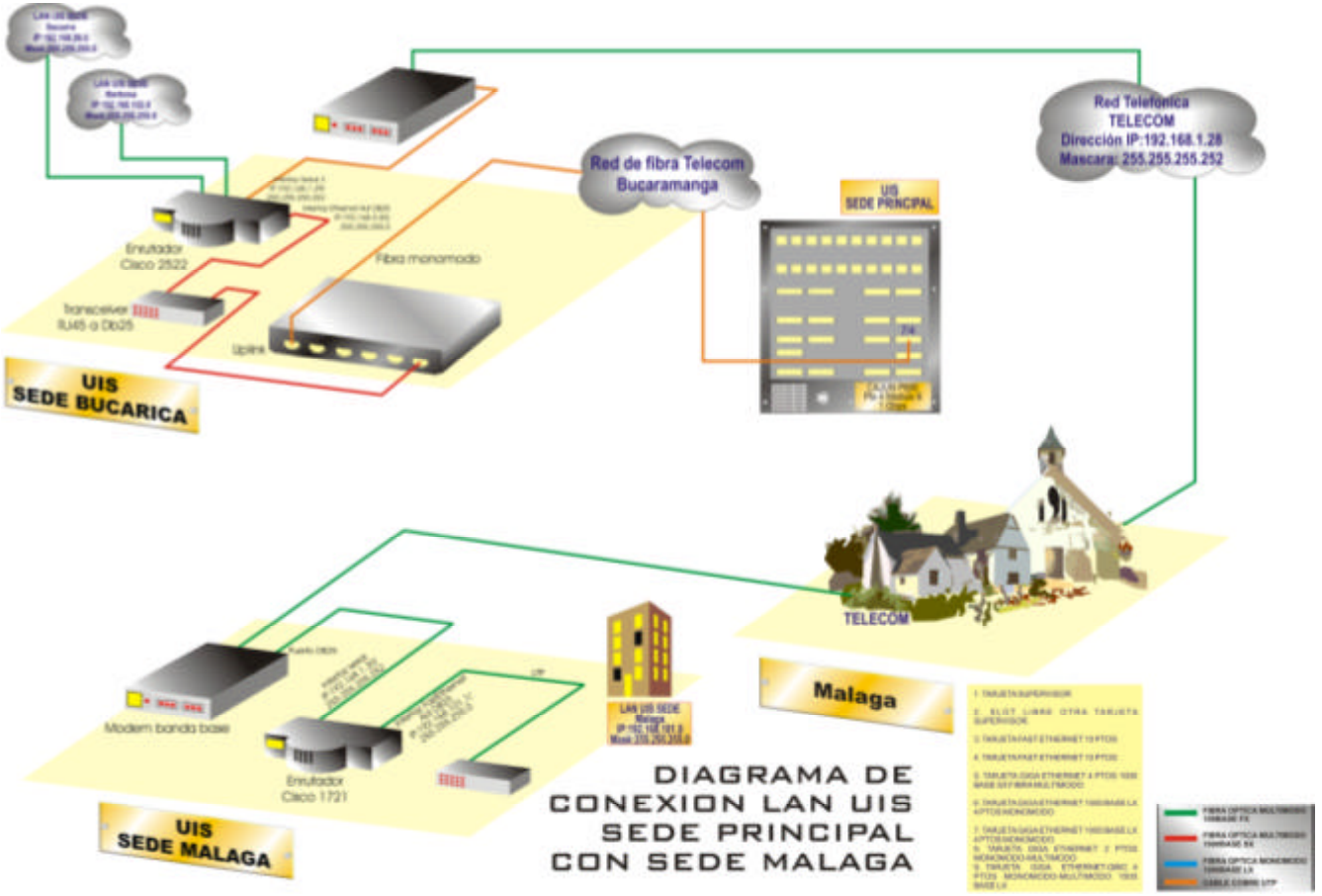
Respecto a los campus sede Barbosa y Málaga también se conectan al switch principal mediante una tarjeta GigaEthernet 1000BASE LX a través de un enlace contratado con TELECOM de 256 Kbps.(Ver Figura 16 y 17).

Figura 16. Conectividad UIS- Campus Barbosa



Fuente: Autor del Proyecto

Figura 17. Conectividad UIS- Campus Málaga



Fuente: Autor del proyecto

Cuadro 9. Conectividad de la TARJETA 8 GIGA-ETHERNET (MONOMODO O MULTIMODO) componente del Switch Avaya modelo Cajun P880 tipo Enterprise

Tarjeta 8	Conectividad de la TARJETA GIGA-ETHERNET (PUEDE SER USADO MONOMODO O MULTIMODO) componente del Switch Avaya modelo Cajun P880 tipo Enterprise	No Tarjeta/ No Puerto
LIBRE		8/1
EDIFICIO INSED		8/2
Total		2

Cuadro 10. Conectividad de la TARJETA 9 GIGA-ETHERNET GBIC (MONOMODO o MULTIMODO) 1000BASE LX ó SX componente del Switch Avaya modelo Cajun P880 tipo Enterprise

Tarjeta 9	Conectividad de la TARJETA GIGA-ETHERNET GBIC (PUEDE SER USADO MONOMODO o MULTIMODO) 1000BASE LX ó SX componente del Switch Avaya modelo Cajun P880 tipo Enterprise	No Tarjeta/ No Puerto
EDIFICIO INGENIERÍA CIVIL-GEOMÁTICA		9/1
EDIFICIO ALA ORIENTAL(División de Servicios de Información-D.S.I)		9/2
LIBRE		9/3
LIBRE		9/4
Total		4

Sistema de cableado de fibra óptica. La fibra monomodo puede acomodar un mayor ancho de banda y permite el tendido de cables de mayor longitud que la fibra multimodo. Debido a estas características, la fibra monomodo se usa a menudo para la conectividad entre edificios mientras que la fibra multimodo se usa con mayor frecuencia para la conectividad dentro de un edificio. La fibra multimodo usa los LED como dispositivos generadores de luz, mientras que la fibra monomodo generalmente usa láser.
La fibra óptica utilizada para la interconexión de los bloques de la Universidad, es en su mayoría de 4 hilos, exceptuando los tramos correspondientes a los edificios de Administración Ala oriental (10 hilos), Biblioteca (6 hilos), Facultad de Salud (8 hilos) y a servidores directamente (2 hilos).

Cada edificio del campus principal esta conectado al Centro de Cableado Principal por un cable de fibra óptica multimodo de 4 hilos, de 62.5/125 micrones, tipo tight buffered para aplicaciones en exteriores, e instalado utilizando ductos subterráneos.

La Facultad de Salud se conecta al Centro de Cableado Principal por un cable de fibra óptica multimodo de 8 hilos, 62.5/125 micrones, tight buffered blindado con protección contra roedores, pasando por las dependencias de la central telefónica del Parque de los Niños de las Empresas Públicas de Bucaramanga,
donde se instaló un repetidor de fibra óptica para corregir la atenuación de la señal, teniendo en cuenta que la distancia hasta la Facultad de Salud es mayor de 2 Km y Ethernet requiere regeneración de la señal sobre fibra óptica para

distancias mayores de 2 Km. Este cable se instaló utilizando los ductos subterráneos telefónicos de las Empresas Públicas de Bucaramanga.

Una vez en la Facultad de Salud, la señal se distribuye a los 5 edificios principales que la conforman, por medio de un hub-repetidor de fibra óptica de 6 puertos, administraba vía SNMP, instalado en el centro de cableado del edificio de Laboratorios y Administración de dicha facultad.

A partir de este hub-repetidor, cada uno de los restantes edificios de la Facultad de Salud se conectan por medio de un cable de fibra óptica de características iguales a los utilizados en el campus principal.

Sistemas de información de la División de Servicios de Información (D.S.I) de la UIS. La Universidad Industrial de Santander como organización de tipo educativo, maneja una serie de procesos complejos dinámicamente interrelacionados, que hacen que la información circulante deba ser administrada en forma ágil y oportuna. Por tal motivo posee una infraestructura de comunicaciones que es la Red de Datos Institucional, centralizada y administrada por la División de Servicios de Información (D.S.I), la cual contiene los principales sistemas de información de la universidad , siendo los de más alto riesgo e impacto informático a nivel organizacional. A continuación se desglosan las principales características de los servidores de la D.S.I como de sus sistemas de información contenidos:

SERVIDOR PELÍCANO. Compuesto por:

Hardware: Es un equipo Silicon Graphics Origin 2000 con las siguientes características:

- Cuatro (4) procesadores risc MIPS r10000 de 300 Mhz
- 4 GB de RAM, arquitectura de memoria compartida
- 48 GB de disco duro
- Una (1) unidad Tape Back Up
- Una (1) unidad CD ROM

Estos servidores presentan un excelente desempeño en tareas que involucran múltiple acceso a los datos y en las aplicaciones que requieren de alta exactitud de cálculo matemático. Son ideales para aplicaciones WEB, servidores de archivos y como servidores para aplicaciones técnico científicas. La serie SGI es altamente actualizable, se puede subir a 8 procesadores MIPS y agregarle componentes hardware como discos duros, unidades de CD ROM, entre otros, debido a su chasis escalable.

Software:

Cuadro 11. Clasificación del Software en el Servidor Pelícano

Sistema Operativo: IRIX 6.5.12. IRIX®6.5 es la quinta generación del sistema operativo SGI® basado en UNIX® y es uno de los más importantes y maduros sistemas operativos UNIX liberados en la industria. IRIX es compatible con la versión UNIX System V Release4.
Software de Aplicación: Informix Dynamic Server 2000. Es un servidor de bases de datos, es decir, es un paquete software que administra los accesos a una o más bases de datos por una o más aplicaciones cliente. La administración de los accesos a las bases de datos incluye actividades como el manejo de concurrencia de peticiones de múltiples clientes, la ejecución de operaciones de lectura y escritura sobre las bases de datos y el mantenimiento de la consistencia física y lógica de los datos. El cliente es un programa de aplicación que un usuario ejecuta para solicitar información a una base de datos. Incluye los programas cliente: INFORMIX-SQL Versión 9.21.UC4: Para la creación y administración de las diferentes Bases de Datos. INFORMIX-4GL Online Versión 7.30.UC4: Para la elaboración y compilación de los programas fuente y objeto a través de los cuales se consigue la interacción con los usuarios, y la administración de la información. Programas Fuente y Objeto: En los diferentes discos duros del servidor se almacenan los programas fuente y objeto, desarrollados para alcanzar la interactividad de los usuarios autorizados con los sistemas de información existentes. Así mismo, se almacenan archivos y reportes generados por los sistemas de información de forma automática o solicitados por los usuarios en su interacción con el sistema.

Fuente: PICO MERCHAN, Benjamín. Ver documentación de la división servicios de información.

Datos: En el servidor Pelícano se encuentran almacenadas las diferentes bases de datos que apoyan la gestión administrativa y académica de la UIS como institución educativa. Es así como las áreas Académicas, Recursos Humanos, Financiera, Biblioteca, Bienestar Universitario, Mantenimiento Tecnológico, Planta Física, entre otras; cuentan con los datos e información almacenados en sus diferentes bases de datos para completar a satisfacción las funciones encomendadas.

Usuarios: Persona que hace uso de alguno de los recursos de cómputo con los que cuenta una organización.

EQUIPOS DE CÓMPUTO. La División de Servicios de Información D.S.I contiene un punto crítico para la universidad que es la sala de servidores que a continuación se reseña:

Cuadro 12. Servidores de la División de Servicios de Información.

Nombre	*Descripción*	*Ubicación*	*Propósito*	*Responsable*
Acreditación		**D.S.I**	**Encargado del proceso de acreditación de la Universidad**	**D.S.I**
Pelícano	**Cuatro (4) procesadores risc MIPS r10000 de 300 Mhz, 4 GB de RAM, arquitectura de memoria compartida, 48 GB de disco duro, Una (1) unidad Tape Back Up, Una (1) unidad CD ROM**	**D.S.I**	**Recurso fundamental que cumple satisfactoriamente funciones académicas, administrativas y financieras. Es el eje principal para las diferentes áreas institucionales de la UIS.**	**D.S.I**
Faisán	**Silicon Graphics, Indigo 2, 128 MB RAM, 4 GB Disco, Iris 5.0**	**D.S.I**	**Desarrollos para el centro de estudios regionales en sistemas de información geográfica ARC-INFO**	**D.S.I**
Cedeuis		**D.S.I**		**D.S.I**
Unired		**D.S.I**		**D.S.I**
Cóndor	**Sun-Sparc 20,Solaris,128 MB RAM,6GB Disco**	**D.S.I**	**Prestar a toda la Comunidad Universitaria todos los servicios para acceso a la Red Internet**	**D.S.I**
DNS		**D.S.I**	**Servidor de Nombres de Dominio de la UIS**	**D.S.I**
Educación Virtual		**D.S.I**	**Desarrollo web de Industrial**	**Ingeniería Industrial**
Halcón	**Silicon Graphics, Crismon, Irix 4.1, 64MB RAM, 2GB Disco.**	**D.S.I**	**Permitir el desarrollo ypuesta en marcha de aplicaciones web de la UIS**	**D.S.I**
Azulejo		**D.S.I**	**Sitios Web UIS**	**D.S.I**
Perdiz		**D.S.I**	**Intranet UIS**	**D.S.I**
Docuware		**D.S.I**	**Manejo de documentación electrónica secretaría general y administración**	**D.S.I**
Bencejo		**D.S.I**	**Reportes Websense**	**D.S.I**
Tyrano		**D.S.I**	**DNS Externo**	**D.S.I**
Aguila	**Prime 4050,8MB RAM, 2.1 GB Disco**	**D.S.I**	**Aplicaciones académicas de las Regionales Barranca, Málaga, Barbosa y Socorro**	**D.S.I**
Dodo		**D.S.I**	**Sitios Web UIS**	**D.S.I**

Fuente: PICO MERCHAN, Benjamín. Ver documentación de la división servicios de información.

SISTEMAS OPERATIVOS CORPORATIVOS. Los sistemas operativos corporativos son los siguientes:

Cuadro 13. Sistemas Operativos utilizados en la UIS

• Unix - Solaris 2.5	• OS/2
• Unix - Irix 4.0 – Irix 6.0	• Windows NT
• Unix - Linux Red Hat 4.0	• Windows 95
• Primos	

Tecnologías Actuales de Seguridad Informática en la UIS. Dentro de las tecnologías de seguridad informática que presenta la UIS tenemos las siguientes:

1. Firewall. La protección de la Universidad está soportado en un sistema integrado hardware/software tipo firewall de marca CISCO modelo PIX 515, más por hardware que por software, es decir es una máquina con sistema operativo propio especializado en funciones de protección firewall.

2. Websense. Fue instalado en el 2001, debido al acelerado crecimiento de la demanda de ancho de banda para acceso a Internet. El primer enlace dedicado a Internet que tuvo la Universidad fue de 128 Kbps, luego se creció a 196 Kbps, 1 Mbps, 2 Mbps, 3 Mbps y a partir de abril del 2003, está en 4 Mbps. Así como ha crecido el tamaño, también ha crecido el costo, actualmente se están pagando alrededor de 10 millones de pesos mensuales por el enlace dedicado a Internet, situación que originó la inquietud de los directivos, más específicamente de los decanos de las diferentes facultades, quienes decían que se estaba pagando mucho por un recurso que se estaba usando mal. Cuando se llegó a 1 Mbps, lo cual significó el salto en costo más alto (se pasó de 2 millones mensuales a 6 millones mensuales), se pidió un mecanismo de control. No era justo que alguien que estuviera consultando algo de tipo académico estuviese compitiendo por el uso de un recurso compartido, con alguien que no estuviese buscando algo académico como deportes, o entretenimiento. La solución consistió en la implantación de un mecanismo para administrar, controlar y optimizar el uso del ancho de banda de acceso a Internet, como lo es el sistema WebSense. Además se hizo necesario también por la imagen de la universidad: debido a que empezaban a surgir comentarios fuera de la Universidad que los estudiantes utilizaban Internet para aspectos no-académicos.

El sistema Websense está contenido en un contrato que se tiene con el proveedor de los equipos principales de la red. Los servidores principales de gestión de la Universidad, o sea los servidores de las aplicaciones informáticas de misión crítica, están bajo un contrato de arrendamiento y soporte con una firma que se llama PROCALCULO S.A, que se encarga de suministrar los servidores principales y el hardware de red necesario para la conexión a Internet. Los servidores más importantes se encuentran en el edificio de administración, son manejados por la División de Servicios de Información de la Universidad y están incluidos en el contrato de arrendamiento con la firma anteriormente mencionada. El contrato incluye el suministro, mantenimiento, asesoría y soporte para el correcto y continuo funcionamiento de los servidores de Bases de Datos, de correo electrónico, de DNS, de Intranet, el enrutador principal de conexión a Internet, el firewall de protección de la red y otros equipos, vitales para la Universidad. El contrato entonces incluye el hardware y el software, incluido el sistema Websense.

3. Protocolo SSH. Secure Shell (SSH), es un software que tiene como objetivo permitir la conexión remota segura a sistemas a través de canales inseguros, también se utiliza para ejecutar órdenes en ese sistema remoto o transferir ficheros desde o hacia él de manera fiable, es por tanto un buen sustituto de órdenes como telnet, ftp o r* de Unix. Todo esto utilizando RSA, SecurID, Kerberos, TIS o la autenticación clásica de Unix (login y password). Entre otras características, ssh también soporta el cifrado automático en sesiones X-Window o modelos de seguridad más avanzados, como el cifrado NFS o la construcción de redes privadas virtuales; su código fuente es libre para uso no comercial (existe otro software casi completamente compatible con ssh y completamente libre denominado OpenSSH) y se puede obtener con http://ssh.fi/. En la actualidad, ssh funciona sobre la mayoría de clones Unix (también existen versiones para Windows y MacOS), y es ampliamente utilizado en todo tipo de entornos, desde universidades a bancos pasando por empresas de cualquier sector.

SSH está formado por un programa servidor, sshd, varios programas cliente (ssh y scp principalmente) y pequeñas aplicaciones para su configuración, como ssh-add, ssh-keygen o ssh-agent. El programa demonio (sshd) se ejecuta en la máquina contra la cual conectamos, mientras que los clientes se han de ejecutar en el sistema desde el cual conectamos.

SSH se utiliza básicamente para iniciar sesiones o ejecutar comandos en un sistema remoto; el otro programa cliente, scp, es utilizado para transferir ficheros entre máquinas, de una forma similar a rcp, lo que por ejemplo permite sustituir el ftp tradicional por este mecanismo.

El cliente conecta al puerto 22 de la máquina servidora y verifica que esta máquina es realmente con la que queremos conectar, intercambia las claves de cifrado entre sistemas (cifradas a su vez, para evitar que un atacante pueda obtener la información) y autentica utilizando .rhosts y /etc/hosts.equiv, RSA o claves de usuario; si todo es correcto, el servidor asigna una terminal virtual (generalmente) a la conexión y lanza un shell interactivo. La UIS emplea este protocolo para proteger la comunicación con Pelícano, que como se expresó anteriormente está dentro de los principales y más importantes servidores de la Universidad ya que maneja los sistemas académicos, financieros y administrativos clasificándose como los más críticos para esta organización.

2.2 EVALUACIÓN DEL RIESGO

La evaluación del riesgo es el proceso total de identificar, cuantificar y minimizar las amenazas que pueden afectar los recursos de un sistema. Como se mencionó en el capítulo anterior una amenaza, es cualquier hecho natural o maniobra de tipo técnico o humana que puede modificar, interrumpir, interceptar o destruir la información de una organización. Se debe tener en cuenta que los riesgos nunca

podrán ser totalmente eliminados: “la seguridad es un proceso no un producto”. Por lo tanto el arte está en no intentar eliminar todos los riesgos, sino administrarlos. La clave para manejar efectivamente los riesgos está en la capacidad para calificar y cuantificar los elementos del riesgo objetivamente hasta reducirlos a niveles aceptables.
El servidor Pelícano es un equipo que se encuentra conectado a la red LAN de la UIS, es accesado diariamente desde diferentes dependencias de la Universidad por sus funcionarios, quienes cuentan con este recurso como una poderosa herramienta en el desempeño de sus labores, pues a través de su servicio dan respuesta a los requerimientos que la UIS demanda para cumplir satisfactoriamente sus funciones académicas, administrativas y financieras. Pelícano es un recurso fundamental para las diferentes áreas institucionales de la UIS, a través del procesamiento de la información almacenada en él se realizan los procesos cruciales asignados a cada una de ellas. Algunos procesos se mencionan a continuación:

- ÁREA ACADÉMICA

Sistema de Información Académico de Pregrado. Entre sus principales aplicaciones se encuentran las siguientes:

- Proceso de selección e ingreso de los aspirantes a los distintos programas académicos ofrecidos por la Universidad, comprende procedimientos como: selección normal de aspirantes, reasignación de cupos, transferencia de estudiantes, readmisión de estudiantes, cambio de programas académicos, simultaneidad de programas académicos, reserva de cupos, ingreso de profesionales.

- Mantenimiento y consulta en línea de la hoja de vida de los estudiantes egresados de la UIS, con datos relevantes como: datos personales, programas académicos cursados, menciones, sanciones, asignaturas homologadas, intercambios.

- Mantenimiento de la información sobre las asignaturas que fueron o son dictadas actualmente en la Universidad, incluye datos como: equivalencia entre asignaturas, áreas de conocimiento.

- Mantenimiento de la información referente a los programas académicos y planes de estudio.

- Proceso de matrícula de estudiantes nuevos y antiguos, proceso de inclusión y cancelación de asignaturas, revisión de matrícula, matrícula cursos de vacaciones, matrículas cursos dirigidos, cancelación de matrícula.

- Proceso de asignación de horarios a los estudiantes y a los docentes. Realiza actividades como: determinación de las asignaturas por grupo, horarios, reservas, manejo de aulas.

- Proceso de generación de certificado de calificaciones. Comprendido por el registro de las evaluaciones a realizar, registro de parciales del período, registro de calificaciones de cursos dirigidos, registro de calificaciones de cursos especiales.

- Proceso para la expedición de documentos tales como constancias de estudios con o sin intensidad horaria, constancia de las asignaturas matriculadas actualmente, constancia de los semestres matriculados, constancia de notas para los egresados, estudiantes activos, retirados de la modalidad presencial y a distancia; además de una serie de certificados que se consideren especiales (constancia de PFU, constancia de estudio para presentar en embajadas, entre otros).

- Proceso para la generación de los certificados académicos, conformado por la generación de los certificados de las asignaturas contenidas en el plan académico, certificado de asignaturas aprobadas por plan académico, duración del programa académico y el número de períodos académicos que ha cursado un estudiante.

- Proceso de Grados. Comprende los procedimientos de verificación de los requisitos para optar al título profesional y los procedimientos para otorgar distinciones a los proyectos de grado.

Sistema de Información Biblioteca. Entre sus principales aplicaciones se encuentran:

- Clasificación y catalogación de los documentos en la base de datos según su tipo (libros, tesis, analíticas y revistas).

- Proceso de préstamo en línea de libros y material bibliográfico a los diferentes usuarios de la biblioteca.

- Proceso de consulta en línea de información sobre el material bibliográfico proporcionado como parámetros de entrada: palabras del nombre del autor, del título o de la materia.

- Proceso para la ejecución de las políticas sobre el manejo de multas y los días de préstamo.

Sistema de Información de Minutas. Permite la generación de los menús que van a ser preparados durante un periodo de tiempo determinado, controlando las calorías y las existencias, de acuerdo a las recomendaciones nutricionales

definidas por la División de Bienestar Universitario para la población que utiliza el servicio. Además, genera el costeo de dichos menús.

- Permite al usuario consultar en línea los menús y reservar el servicio para un determinado día. El sistema controla que dichas cantidades no excedan la oferta teniendo en cuenta lo ya vendido.

- Elaboración de la minutas diarias tanto para comedores como cafetería, generando los reportes de: recetas a utilizar, alimentos a pedir, etc.

Sistema de Información de Comedores

- Permite el establecimiento de los parámetros de evaluación a ser tenidos en cuenta para realizar la asignación del servicio de comedores a lo estudiantes que lo solicitan.

- Permite registrar los datos básicos para la solicitud del servicio. Valida para cada solicitud el cumplimiento de ciertos requisitos académicos y financieros (los cuales son tomados directamente de dichos sistemas con el fin de asignar o rechazar la solicitud.

- Genera los reportes inscritos, asignados, rechazados, recibos de pago y arqueo entre otros. Genera estadísticas por servicio, usuarios, estrato, prioridad, etc.

- AREA ADMINISTRATIVA

Sistema de Información de Recursos Humanos. Entre sus principales aplicaciones se encuentran las siguientes:

- Mantenimiento y consulta en línea de la hoja de vida, hoja de pagos y situaciones administrativas de los empleados vinculados a la UIS en sus diferentes modalidades: Personal de Planta, Jubilados y Sustitutos, Docentes de Cátedra, Servicios Prestados, Aprendices Sena, Auxiliaturas y Becas de Postgrado.

- Generación de listados en los cuales se proporciona información acerca de la planta de cargos actual de la Universidad, los cargos base y actuales de los empleados, los cargos vacantes y los NNs.

- Proceso de liquidación mensual de nómina y liquidación periódica de primas y mesadas adicionales para los empleados en sus diferentes modalidades de contratación.

- Proceso de cálculo de ajuste de sueldo de acuerdo a: los porcentajes de retroactivo autorizados por el gobierno nacional, la asignación de los diferentes

puntajes, cambios en la escala salarial o en el cargo desempeñado por el empleado.

- Generación de los reportes de autoliquidación y medios magnéticos dirigidos a las EPS, AFP y ARP de las cuales forma parte el empleado.

- Generación de listados con información relevante y concisa acerca del manejo administrativo de la Universidad, requerida por instituciones gubernamentales y académicas como son la DIAN, el Ministerio de Hacienda y el ICFES entre otros.

- Generación de reportes estadísticos con información importante para las dependencias de la UIS como Rectoría, Planeación, Recursos Humanos, Financieros; para apoyar la toma de decisiones administrativas.

Sistema de Información de Mantenimiento Tecnológico

- Permite el control de las Unidades Académico administrativas sobre los equipos asignados a ellas.

- Permite incluir en línea la información básica y técnica que describe un equipo.

- Permite a las Unidades Académico Administrativas generar solicitudes de servicio o asesorías para un concepto determinado.

- Genera los reportes pertinentes a las solicitudes de servicio y cumplimiento de estas.

- AREA FINANCIERA

Sistema de Información Financiero. Entre sus principales aplicaciones se encuentran:

- Permite realizar la programación, adición, traslados y ejecución presupuestal. Controla la emisión y ejecución de C.D.P, proyección de compras, consultas y reportes presupuestales.

- Posibilita el registro en línea de las cuentas por cobrar por: facturación de servicios, aportes, matrícula de estudiantes, genera las facturas de venta, recibos de liquidación de matrícula y controla la Cartera.

- Registra el manejo de caja, bancos, préstamos bancarios, prestamos entre Unidades Académico Administrativas, entre fondos y traslados bancarios.

- Permite el mantenimiento de la información del catálogo de elementos, los proveedores, ordenadores de gastos, inversiones, importaciones, cajas menores, fondos fijos, ordenes de compra, de trabajo y de servicio.
- Permite el registro en línea de las cuentas a pagar recibidas en tesorería, activa las cuentas a pagar, asigna cheques e imprime los cheques girados. Genera los reportes de las transacciones recibidas de Tesorería Presupuesto: cuadre de comprobantes, movimientos y saldos, libros oficiales, libros auxiliares y estados financieros.

- Proceso de generación de las órdenes de pago para los empleados y los diferentes proveedores de la UIS.

- Generación de reportes dirigidos a las dependencias administrativas de la UIS y a entidades gubernamentales tales como el Ministerio de Hacienda, la DIAN, etc.

Sistema de Información de Costos Universitarios

- Permite la captura y actualización de las constantes que se utilizan como información básica para los procesos de costos universitarios.

- Genera los cuadros de costos tomando la información requerida desde los Sistemas de Información de Recursos Humanos, Académico y Financiero, entre los cuadros de costos generados se encuentran los siguientes: Resumen del gasto de la institución por funciones según detalle del gasto, Matriz de recursos y servicios de las Unidades Académicas, Resumen del gasto semanal de la institución por funciones y programas según detalle del gasto, Gastos semanales directos, de apoyo y totales por actividades de las unidades de docencia, Costo total semanal de docencia estudiante/hora por programa académico, Costo total de docencia por alumno según programa académico, gasto directo gasto de apoyo y gasto total semestral por funciones de la institución.

Por lo tanto, para este tipo de organización de tipo educativo es de vital importancia mantener en perfecto estado y funcionamiento el servidor de bases de datos Pelícano, como también mantener la información totalmente confiable, íntegra y disponible para ser consultada en cualquier momento que sea requerida. Es así como el servidor Pelícano es un punto crítico para la seguridad de la Universidad Industrial de Santander.

2.2.1 Análisis de riesgos en los activos organizativos y medidas de contención. Luego de identificar los activos organizativos o recursos informáticos de la UIS, los cuales son los que se deben proteger, este apartado pretende determinar las amenazas y vulnerabilidades a las que están expuestos los recursos, como también el análisis de tener el recurso inaccesible o destruido, proceso que se realiza mediante el análisis de riesgos.

- ANÁLISIS DE RIESGOS INFORMÁTICOS. Es el proceso que permite identificar, analizar, administrar y evaluar las fuentes de riesgos antes de que amenacen el funcionamiento continuo y confiable de los sistemas de información, permitiendo además comparar dichos riesgos con el costo de las medidas de prevención, con el objeto de tomar decisiones adecuadas al respecto.

Este análisis requiere identificar previamente los activos de la organización para poder así, cuantificar o cualificar los riesgos para cada tipo de activo, además del valor del activo, y el impacto potencial de incidentes de seguridad en la Organización.

La información que se puede obtener al efectuar un análisis de riesgos es:

- Determinación precisa de los recursos sensibles de la organización.
- Identificación de las amenazas del sistema.
- Identificación de las vulnerabilidades específicas del sistema.
- Identificación de posibles pérdidas.
- Identificación de la probabilidad de ocurrencia de una pérdida.
- Derivación de contramedidas efectivas.
- Identificación de herramientas de seguridad.
- Implementación de un sistema de seguridad eficiente en costes y tiempo

En un proceso de análisis de riesgos se maneja la siguiente terminología:

ACTIVOS. Son aquellos componentes de la organización (tangibles e intangibles) que son parte del patrimonio de la misma y necesitan ser resguardados.

AMENAZAS. Se definen como “los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos”. La amenazas se pueden materializar y transformarse en agresiones.

VULNERABILIDADES. Se define como “la ocurrencia real de materialización de una amenaza sobre un activo”, la vulnerabilidad es una propiedad de la relación entre un activo y una amenaza. Hace sistemas más propensos de ser atacados por una amenaza o hace que un ataque tenga una mayor probabilidad de tener éxito.

IMPACTO. Se define como el “daño producido a la organización por un posible incidente” y es el resultado de la agresión sobre el activo”. El Impacto puede ser cuantitativo (si representa pérdidas cuantitativas monetarias directas o indirectas); cualitativas con pérdidas orgánicas (por ejemplo daño de personas y cualitativo con pérdidas funcionales.

RIESGO. Se ha definido como la “posibilidad de que se produzca un impacto dado en la organización”.

El análisis de riesgos es el producto del análisis organizado sobre los elementos anteriores (activos, amenazas, vulnerabilidades e impactos) que se refleja en un indicador resultante de la combinación de la vulnerabilidad y el impacto que procede de la amenaza actuante sobre el activo.

En el proceso de análisis de riesgos es importante tener en cuenta la ecuación del riesgo:

$$(1) \quad B > P * L \text{ donde:}$$

B: Peso o carga que significa la prevención de una pérdida específica.
P: Probabilidad de ocurrencia de una pérdida específica.
L: Impacto total de una pérdida específica.
Dicha relación nos orienta acerca de cuándo y cuánto invertir en tal proceso, ya que si:

$$B \leq P * L$$

Nos indicaría que debemos implementar una medida de prevención, pero si:

$$B > P^* L$$

En tal caso no sería necesaria una medida de prevención.

Lo anterior es el resultado del análisis de la ecuación del riesgo, ya que si observamos la efectividad del coste, es decir, el control (B) ha de tener menos coste que el valor de las pérdidas debido al impacto de ésta si se produce el riesgo temido, debido a una ley básica que dice: el costo del control ha de ser menor que el activo que protege.

Respecto al Impacto o factor (L) en la ecuación de riesgo (1), es difícil evaluarlo, debido a que este incorpora daños a la información, equipos, pérdidas por reparación, por levantar el sistema y pérdidas por horas de trabajo, provocando que sea muchas veces la apreciación subjetiva del personal de la organización la que lo establezca.

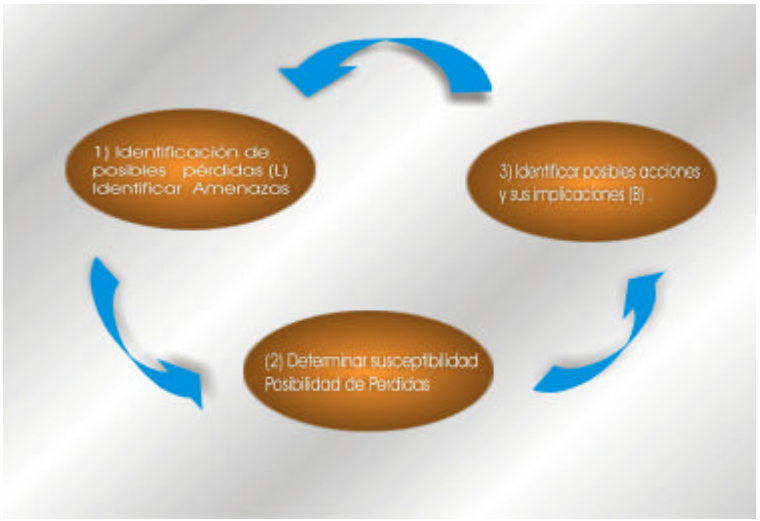
La probabilidad de ocurrencia de una pérdida o factor (P), está relacionada con la determinación del impacto total (L), que depende del entorno en el que esté la posible pérdida. La probabilidad puede asociarse a una tendencia o frecuencia conocida.

Conocido (P) para un (L) dado, se obtiene la probabilidad de pérdida relativa de la ocurrencia P*L que se comparará con (B), que indica el peso que supone implantar la medida de prevención respectiva. Resumiendo, el factor (B) expresa lo que se requiere para prevenir una pérdida. Por ejemplo, el peso o carga de

prevención para que un vehículo no se quede sin gasolina es el costo de echarle gasolina. El peso incluye los valores de tiempo y costo: ir a la gasolinera, esperar a que esté libre un surtidor, poner gasolina y pagar, pero ¿Cuánta protección (B) sería necesaria? ó ¿Cuánta gasolina debería echarse en el tanque?, la respuesta sería hasta dónde se quiera desplazar el coche.

Se trata de encontrar a cuánto puede ascender nuestro presupuesto en materia de seguridad (B) si conocemos el impacto económico (L) que eso supone y hemos especificado un factor de probabilidad (P) de que esta catástrofe ocurra. Por lo tanto si $B \leq P^* L$ instalamos las medidas.

Figura 18. Pasos para el análisis de riesgos



Fuente: RAMIÓ, AGUIRRE.J. (2002). *Curso de Seguridad Informática*. Material Docente de libre distribución.

RIESGOS, DECISIÓN E INCERTIDUMBRE. Todo proyecto relacionado con Riesgos (y entre ellos los relativos al Análisis y Gestión de Riesgos para manejar o gestionar la Seguridad de sistemas de información) tienen como objetivo central una toma de decisión específica y consisten en preparar la consecución de dicho objetivo lo más eficiente y eficazmente posible. La decisión a tomar es la acción de neutralizar un riesgo no aceptable y se plasma en la implantación de funciones y mecanismos de salvaguarda, que es una acción a elegir entre alternativas de acciones distintas y más o menos excluyentes entre sí.

Esta decisión es obligada: el actor que decide o 'decisor' se ve forzado a 'jugar' o sea elegir entre líneas alternativas de acción posibles (incluida la inacción) y realiza la 'mejor apuesta' posible con la información disponible, tanto si después gana como si pierde (o sea consiga o no el objetivo real de reducción de riesgo que subyace a la decisión tomada).

La toma de decisión requiere manejar información previa, organizada en un sistema de información 'directivo' o de ayuda a la decisión. La Gestión de Riesgos de los Sistemas de Información se caracteriza por tener que tomar decisiones con alto nivel de 'incertidumbre' (o sea falta de información en zonas más o menos amplias). Esta incertidumbre se debe a:

- La falta de 'series' históricas en la información utilizada.
- La experiencia limitada sobre los problemas relativos a riesgos.
- La poca madurez comercial de los métodos disponibles para su solución.
- La propia idiosincrasia de los conceptos manejados.

Para varios estudiosos de este tema, la incertidumbre sobre la información para la decisión requiere trabajar con algún tipo de 'probabilidades', sean objetivas o subjetivas y se formulen explícitamente o no. Otros autores no admiten esa relación necesaria entre probabilidades y decisión si hay elementos no identificables o enumerables en el conjunto de informaciones que soportan las acciones alternativas: la incertidumbre se encuentra, no ya en probabilizar los estados naturales, sino en no poder identificarlos o enumerarlos completamente.

Los proyectos de seguridad, inmersos en esa situación generalizada de alta incertidumbre incorporada en diversos aspectos y niveles, soportan la adopción de diversos mecanismos específicos tales como:

- Técnicas de conducción de un proyecto de tratamiento de riesgos (para reducir su propio riesgo de no alcanzar su terminación).

- Las técnicas utilizables en un proyecto de tratamiento de riesgos pertenecen a la familia de Técnicas de Ayuda a la Decisión con incertidumbre.

TÉCNICAS DE CONDUCCIÓN DEL PROYECTO. La incertidumbre elevada que comporta todo proyecto de Análisis y Gestión de Riesgos promueve dos tipos de medidas generales en la conducción de un proyecto de seguridad:

- El desarrollo de dicho proyecto en forma iterativa[12].

[12] El desarrollo iterativo promovido en la Introducción de la Guía de Procedimientos de MAGERIT también se recomienda en la Guías internacionales ISO/IEC para la Gestión de la Seguridad de los Sistemas de Información (GMITS, referencia ISO/IEC JTC 1/SC 27 N 1231, PDTR 13335-3, versión de 22.3.1996): "Se aconseja empezar considerando un Análisis de Riesgos de alcance estratégico corporativo. Esta opción recomendada implica la realización de un Análisis de Riesgos global para todos los Sistemas de Información que permita identificar rápidamente los sistemas que están sometidos a riesgos elevados. Se prosigue aplicando por un lado las normas básicas de seguridad para los dominios que no tengan riesgos elevados, mientras que para éstos se realizan Análisis de Riesgos detallados. De esta manera las etapas del análisis pueden enfocarse donde están los riesgos reales".

▪ Una vigilancia o control especialmente frecuentes y profundos en los hitos de seguimiento y decisión del proyecto para evitar los desvíos respecto a su objetivo.

- TIPO DE TÉCNICAS DE DECISIÓN USADAS EN EL ANÁLISIS Y GESTIÓN DE RIESGOS

Existen una gran familia de técnicas usadas en el análisis y gestión de riesgos, las cuales pueden tomar dos enfoques[13] que abarcan el panorama de los diferentes tipos, envergaduras y certidumbres de los proyectos de Análisis y Gestión de Riesgos que se van a encontrar normalmente con cierta frecuencia.

- El primer enfoque plantea sólo técnicas de apoyo ligero al experto, que es quien va preparando y tomando todas las decisiones necesarias para realizar las tareas esenciales del proyecto.

- El segundo enfoque plantea 'técnicas expertas' (de ayuda a la decisión) que requieren más esporádicamente la intervención del experto, preparando y tomando buena parte de las decisiones necesarias para realizar las tareas esenciales del proyecto.

El primer enfoque se apoya en las técnicas matriciales y algorítmicas sencillas que va seleccionando y engarzando el experto. En el segundo enfoque ciertas técnicas seleccionan y engarzan las Técnicas sencillas del enfoque anterior.

No conviene olvidar una contradicción implícita en toda técnica de ayuda a la decisión. Las técnicas expertas del segundo enfoque paradójicamente suelen ser más fáciles de manejar cuanto más sofisticadas (se construyen precisamente para reducir la necesidad de expertos humanos) pero en compensación sus premisas y resultados son más difíciles de interpretar por no-expertos.

- DECISIÓN APLICADA AL RIESGO

Incertidumbre en la Información o sólo en su contexto relacional. La Teoría de la Decisión establece una clasificación general de métodos y criterios de ayuda a la decisión. En cada nodo de decisión del problema debe haber un conjunto de informaciones que soportan las acciones potenciales alternativas previas a la decisión:

1. Los elementos del conjunto no son identificables o se ignoran:

a. Totalmente: entonces la incertidumbre es absoluta y no hay decisión posible.

[13] Según la Metodología de Análisis y Gestión de riesgos de los sistemas de información MAGERIT.

b. En parte: entonces la incertidumbre existe en el sentido de plausibilidad y se tienen que emplear técnicas de *lógica difusa.*

2. Los elementos del conjunto son identificables. Entonces la incertidumbre depende del contexto relacional entre esos elementos; si éste es:

a. Determinado: no hay incertidumbre y se emplean técnicas de cálculo algorítmico (no hay decisión en sentido estricto, sino determinación).

b. Aleatorio: la probabilidad de cada alternativa es conocida y se pueden emplear técnicas de cálculo probabilístico (tampoco hay decisión).

c. Incierto parcialmente: (incertidumbre 'distributiva'), es decir se conoce cierta distribución no probabilística de potencialidades y se suelen emplear técnicas de decisión bajo criterios diversos (pesimista, frustración ...) o de decisión bayesiana.

d. Incierto totalmente: (incertidumbre 'no distributiva'), hay posibilidad (no cuantificable) y se emplean técnicas de simulación.

e. Hostil: los adversarios toman decisiones y se emplean técnicas de ***juegos***.
Para seleccionar las técnicas de decisión más adecuadas a los problemas de seguridad, hay que identificar las entidades y los conceptos del Modelo de Análisis y Gestión de Riesgos que son homologables respectivamente, tanto al conjunto de informaciones soporte de las alternativas entre las que se toma la decisión, como al contexto relacional de ese conjunto:

- El conjunto de las informaciones de soporte a las acciones alternativas potenciales está constituido por los niveles de agresión, o bien de vulnerabilidad combinada de amenaza y activo vulnerable. Estos niveles de agresión forman un conjunto identificable, lo que excluye incertidumbres de tipo absoluto (que no permiten tomar ninguna decisión racional) o plausibilidades (y sus técnicas de lógica difusa*).*

- El contexto relacional de las informaciones de vulnerabilidad del activo a la amenaza puede ser de tipos diversos y comprende en principio todos los citados: determinado, aleatorio, incierto parcialmente, incierto totalmente y hostil.

- LA PROSPECTIVA EN EL ANÁLISIS DE RIESGOS INFORMÁTICOS

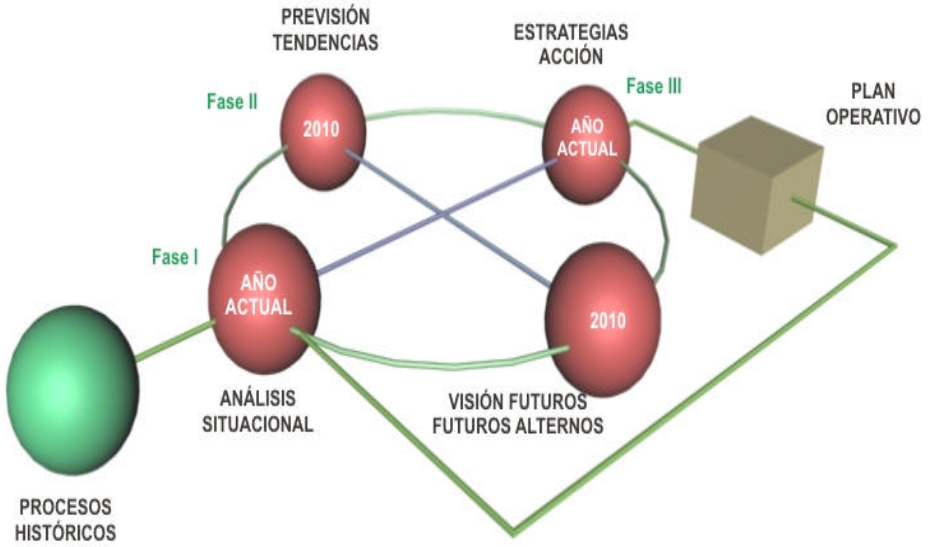
La prospectiva es un acto creativo, que encierra además elementos de cambio y transformación, pero ante todo es una opción que invita a asumir una actitud activa hacia el mañana, además de permitir impulsar el futuro, puede aportar ingredientes muy importantes en la planeación y toma de decisiones, ya que identifica peligros y oportunidades de determinadas situaciones futuras y ofrece

políticas y acciones alternativas aumentando así el grado de elección, estas bondades de la prospectiva son los elementos que el autor del proyecto observó y piensa puede ser utilizados como una metodología para realizar el análisis de riesgos informáticos. Es conveniente anotar que muchas organizaciones de hoy en día desconocen el valor de la prospectiva, prefiriendo jugar muchas veces con hipótesis preestablecidas que pocas veces suceden y/o aplicar lo que se llamaría una estrategia reactiva o del bombero, la cual consiste en actuar cuando ya se produce la crisis, improvisando constantemente, sin comprender que cuando la velocidad y el ritmo de los cambios es tan grande, las acciones realizadas por las organizaciones, sin una acción prospectiva previa, pueden ocasionar acciones ciegas con consecuencia irreparables. Si hablamos de prospectiva tecnológica, de lo que se trata es de hacer énfasis en los problemas tecnológicos de ciertos sistemas sociales y/o áreas tecnológicas en las empresas para diseñar escenarios a futuro para el desarrollo de las mismas, como en nuestro caso la problemática surgida en las organizaciones a raíz de la seguridad informática

- MÉTODOS PROSPECTIVOS

La figura muestra esquematizada la metodología de la prospectiva.

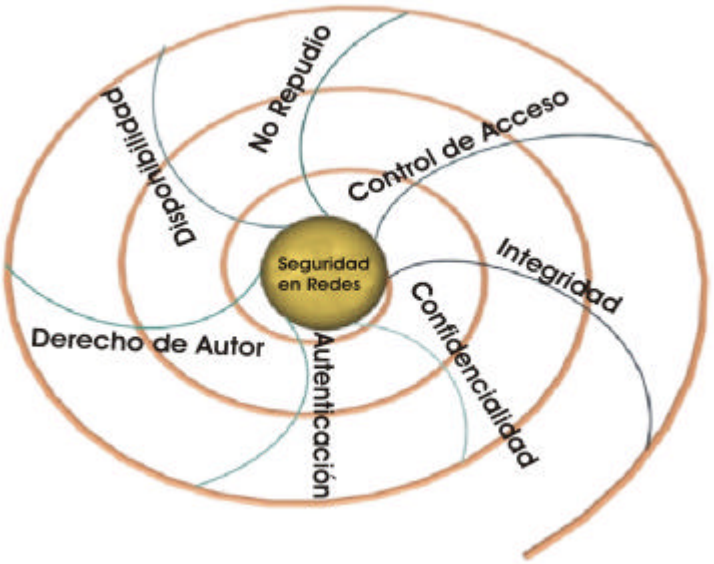
Figura 19. Fases de la Prospectiva



Fuente: MARTELO, GÓMEZ, R. MOSQUERA ROBBINS, F. (2004) *Sistema de gestión para toma de decisiones en pymes, basado en prospectiva y cuadro de mando integral*. Miembros del Grupo de Investigación en Innovación y Organización de Procesos Empresariales.

- Análisis Estructural de Variables. Todo sistema se presenta como un conjunto de elementos relacionados entre si. La estructura del sistema, es decir, la red de las relaciones entre sus elementos, siempre será esencial para comprender su evolución, puesto que la misma conserva cierta permanencia [14]. Como se observa en la siguiente figura:

Figura 20. La seguridad en Redes de Telecomunicaciones como Sistema.



Fuente: Autor del Proyecto

Por lo tanto el análisis estructural es un instrumento de estructuración de ideas que posibilita la descripción de un sistema mediante una matriz que relaciona todos sus elementos constitutivos, y a través de su estudio se evidencian las variables claves para la evolución del propio sistema[15].

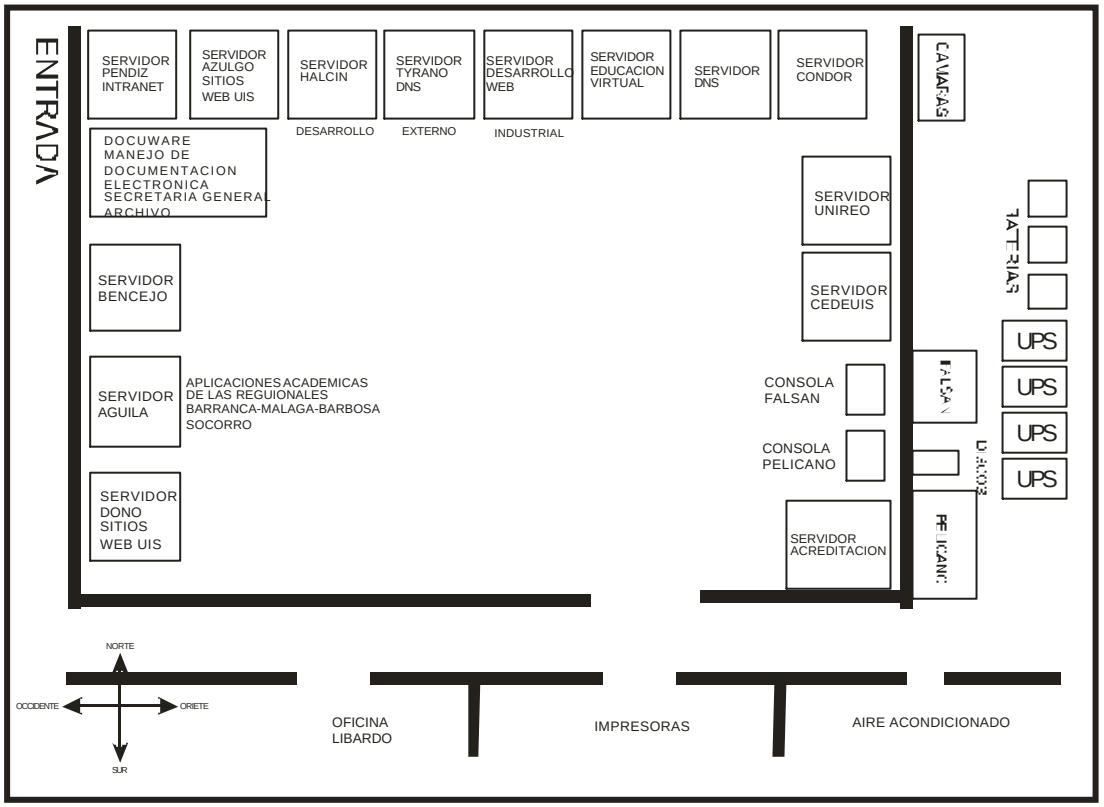
Para nuestro caso de estudio se propone para efectuar el análisis de riesgos la metodología prospectiva llamada “Análisis Estructural de Variables” compuesta por tres fases que son: identificación de las variables, localización de las relaciones en la matriz del análisis estructural y por último la búsqueda de las variables claves a través del método MICMAC, las cuales fueron desarrolladas en la siguiente forma:

a. Identificación de Variables. Para la UIS el punto más crítico y delicado es la División de Servicios de Información (D.S.I), pero en especial la sala de servidores la cual se muestra a continuación en la (figura 21) y en la que se efectuó un

[14] Godet Michel.(2000): La caja de Herramientas de la prospectiva estratégica .
[15] Gabiña,J(1998). La prospectiva una herramienta cargada de futuro. Editorial Prentice Hall

diagnóstico del estado de la seguridad informática de la UIS, con la intención de analizar la evolución de la misma desde el pasado al presente respecto a amenazas y ataques sufridos, como a las posibles tendencias futuras en cuanto debilidades potenciales con el fin de poder responder adecuadamente al estado futuro del sistema. Para la determinación de las variables, se realizaron encuestas con personal experto de la División de Servicios de Información como de otros puntos de la UIS, además de reuniones con el Ing. MsC Benjamín Pico Jefe de Seguridad de la UIS quien aportó a esta investigación todo su conocimiento y colaboración.

Figura 21. Sala de Servidores División de Servicios de Información



Fuente. Autor del Proyecto

Luego se elaboró un listado de variables o problemas que han afectado o pudieran afectar al sistema constituido por la seguridad informática y su contexto, del cual se extractaron las siguientes:

Seguridad Física y Ambiental

1. Fluctuaciones en la tensión o frecuencia en el suministro de energía.
2. Daño en componentes hardware.
3. Elevada temperatura de servidores
4. Incendio
5. Acceso físico

Sistema Operativo

6. El sistema de ficheros
7. Permitir montar y desmontar sistemas de ficheros a los usuarios
8. Los bits setuid y setgid

Debilidades de los servicios web disponibles en el servidor Pelícano

9. Daytime: Time of Day, puerto TCP 13
10. Time: Puerto TCP 37
11. FTP (File Transfer Protocol): puerto TCP 21
12. Telnet: puerto TCP 23
13. SMTP (Simple Mail Transfer Protocol): puerto TCP 25
14. Finger: puerto TCP 79
15. rexec: puerto TCP 512
16. rlogin: puerto TCP 513 y rsh: puerto TCP 514
17. NFS (Network File System): puerto TCP 2049

Puertos UDP abiertos:

18. RPC (Sun Remote Procedure Call) : Puerto UDP 111
19. SNMP (Simple Network Management Protocol): puerto UDP 161
20. Syslog: Puerto UDP 514
21. Identificación de direcciones IP-Servidores UIS

Debilidades encontradas en el Firewall de la UIS (Amenazas externas)

22. Exploración de puertos al Firewall de la UIS y routers ETB y TELECOM

Debilidades en los servidores de correo de la UIS.

23. Violación del Websense
24. Violación de los servidores de correo de la UIS.

Debilidades Software de Aplicación, Programas fuente y objeto:

25. Alteración malintencionada del software de aplicación, virus, caballos de Troya u otros.

Debilidades encontradas en los datos:

26. Divulgación, modificación, interceptación, pérdida total o parcial de los datos.

Debilidades encontradas en los usuarios:

27. Atacante interno. Sistema de autenticación de UNIX, revelado de contraseñas.

b. Localización de las relaciones en la matriz del análisis estructural. En esta etapa se definen las relaciones entre las variables o problemas seleccionados, mediante una matriz de doble entrada la cual determinará las relaciones directas ó no, dependiendo si toma valor de 3 ó 0 respectivamente. Es conveniente resaltar que la matriz mostrada a continuación es la resultante de las matrices analizadas por los expertos[16] y cuyos datos fueron introducidos y procesados apoyándonos en un software francés llamado LIPSOR[17] que aplica este método prospectivo: análisis estructural de variables. (Ver cuadro 13).

Cuadro 14. Matriz de relaciones entre variables- Matriz de influencias directas (MID).

	1: FlucElec	2: FallHardw	3: ElevTemp	4: Incendio	5: AccFis	6: SistFiUnix	7: MonDemFi	8: bitssetuid	9: Daytime	10: Time	11: ServFtp	12: Telnet	13: SMTP	14: Finger	15: Rexec	16: rlogin	17: NFS	18: RPC	19: SNMTPUd	20: SyslogUd	21: Ident-IP	22: ExpPtoFir	23: VioWebse	24: VioCondAl	25: AltSofVir	26: DivperDat	27: AtacInter
1 : FlucElec	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2 : FallHardw	3	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3 : ElevTemp	3	3	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4 : Incendio	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5 : AccFis	0	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
6 : SistFiUnix	0	0	0	0	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	3	3
7 : MonDemFi	0	0	0	0	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	0	3	3
8 : bitssetuid	0	0	0	0	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	0	3	0
9 : Daytime	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10 : Time	0	0	0	0	3	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11 : ServFtp	0	0	0	0	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	0	3	0	0	0
12 : Telnet	0	0	0	0	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3
13 : SMTP	0	0	0	0	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	0	0	3
14 : Finger	0	0	0	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	0	3	0	3	3
15 : Rexec	0	0	0	0	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	0	3	3	0	3
16 : rlogin	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3
17 : NFS	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	0	3	3
18 : RPC	0	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3
19 : SNMTPUd	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3
20 : SyslogUd	0	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	0	3	3
21 : Ident-IP	0	0	0	0	3	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	0	3	3
22 : ExpPtoFir	0	0	0	0	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	0	3	3
23 : VioWebse	0	0	0	0	0	0	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3
24 : VioCondAl	0	0	0	0	0	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3	3
25 : AltSofVir	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	3	3
26 : DivperDat	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	3
27 : AtacInter	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0

Fuente: Software francés de Análisis Estructural de Variables. LIPSOR – EPITA – MICMAC.

La matriz muestra la influencia directa potencial o no de cada una de las variables con respecto a las otras así:

0 : Poca o ninguna influencia directa potencial.
3 : Alta influencia directa potencial.

[16] El grupo de expertos estuvo conformado por: Ing MsC Benjamín Pico Merchan: actualmente administrador de la red de datos institucional de la Universidad, Ing José de Jesús León Pereira: Especialista en Telecomunicaciones y docente de la UIS, MsC (C) Raul Martelo Gómez: Especialista en Telecomunicaciones UIS y Miembro del Grupo de Investigación en Innovación y Organización de Procesos, Ing. Oscar Mauricio Parra: Especialista en Telecomunicaciones UNAB.

[17] Disponible en http://www.3ie.org/lipsor/plan.htm

La tabla presenta la cantidad de 0 y 3 de la matriz como la tasa de motricidad calculada como el cociente entre la cantidad de valores diferentes de 0 entre el número total de valores o celdas de la matriz.

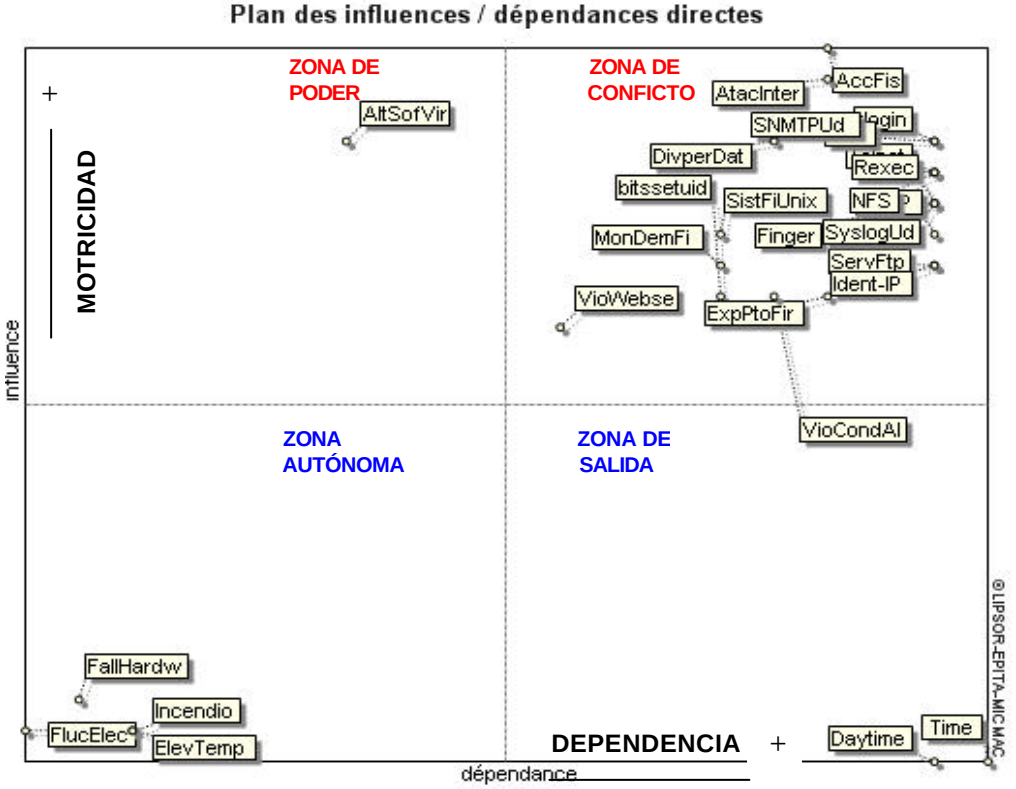
Cuadro 15. Indicadores Matriz de influencias directas (MID).

INDICADORES	VALORES
Tamaño del matriz	27
Número de iteracciones	2
Número de ceros	267
Número de unos	462
Total	462
Tasa de motricidad	63,37449%

Fuente: Software francés de Análisis Estructural de Variables. LIPSOR – EPITA – MICMAC.

c. Búsqueda de las variables claves a través del método MICMAC: El objetivo del análisis es interpretar el conjunto de problemas en función de su posición en cada uno de los cuadrantes los cuales representan las zonas de poder, conflicto, salida y autonomía como se muestra en la figura 22 a continuación:

Figura 22. Gráfico Motricidad vs Dependencia



Fuente: El método MICMAC fue creado por Michel Godet. El software es francés y fué desarrollado por LIPSOR - Cf M.Godet, Manual de prospectiva estratégica, Tomo 2 Edición Dunod 2001 - Cf M.Godet, Creación de futuros escenarios de planeación como herramientas de dirección estratégica, Ediciones Económica.

Los problemas ubicados en la zona de poder se caracterizan por presentar motricidad alta y baja dependencia; significa que las acciones que se derivan de ellas tienen la capacidad de influir significativamente en el comportamiento del sistema.

Para el caso analizado el problema aumentó con la variable identificada con el número 25, por lo tanto se les asignó un valor de riesgo alto, dentro de las cuales están:

- Amenaza 25: Alteración malintencionada del software de aplicación, mediante la inclusión dentro del código de programas que se instalan como: virus, caballos de Troya u otras amenazas.

Los problemas ubicados en la zona de conflicto se caracterizan por presentar alta motricidad y dependencia, significa que las acciones que se deriven de ellos tienen la capacidad de generar situaciones conflictivas en el comportamiento del sistema.

Para el caso analizado se encuentran en esta zona las variables identificadas con los números: 5,6,7,8,11,12,13,14,15,16,17,18,19,20,21,22,23,24,26 y 27, a las cuales se les asignó un valor de riesgo medio y corresponden a:

- Amenaza 5: Acceso físico
- Amenaza 6: El sistema de ficheros
- Amenaza 7: Permitir montar y desmontar sistemas de ficheros a los usuarios
- Amenaza 8: Los bits setuid y setgid
- Amenaza 11: FTP (File Transfer Protocol): puerto TCP 21
- Amenaza 12: Telnet: puerto TCP 23
- Amenaza 13: SMTP (Simple Mail Transfer Protocol): puerto TCP 25
- Amenaza 14:Finger: puerto TCP 79
- Amenaza 15: rexec: puerto TCP 512
- Amenaza 16: rlogin: puerto TCP 513 y rsh: puerto TCP 514
- Amenaza 17: NFS (Network File System): puerto TCP 2049
- Amenaza 18: RPC (Sun Remote Procedure Call) : Puerto UDP 111
- Amenaza 19: SNMP (Simple Network Management Protocol): puerto UDP 161
- Amenaza 20: Syslog: Puerto UDP 514
- Amenaza 21: Identificación de direcciones IP-Servidores UIS
- Amenaza 22: Exploración de puertos al Firewall de la UIS y routers ETB y TELECOM
- Amenaza 23: Violación del Websense
- Amenaza 24: Violación de los servidores de correo de la UIS.
- Amenaza 26: Divulgación, modificación, interceptación, pérdida total o parcial de los datos.

- Amenaza 27: Atacante interno. Sistema de autenticación de UNIX, revelado de contraseñas.

Los problemas que se ubican en la zona de salida, se caracterizan por presentar baja motricidad y alta dependencia, el cual significa que son altamente influenciados por las acciones derivadas de los problemas ubicados en las zonas de poder y de conflicto.

Para el caso analizado se encuentran en estas zonas las variables 9 y 10, a las que se les asignó un valor de riesgo un valor de riesgo bajo.

- Amenaza 9: Daytime: Time of Day, puerto TCP 13
- Amenaza 10: Time: Puerto TCP 37

Los problemas que se ubican en la zona autónoma se caracterizan por presentar baja motricidad y baja dependencia; se muestran como pocos determinantes en el comportamiento del sistema. Debido a que las variables identificadas con los números 1,2,3 y 4 se presentan en esta zona, se concluye que dicho aspecto no es muy determinante para el sistema, por lo que se les asignó un valor de riesgo bajo, para nuestro caso sería:

- Amenaza 1: Fluctuaciones en la tensión o frecuencia en el suministro de energía.
- Amenaza 2: Daño en componentes hardware.
- Amenaza 3: Elevada temperatura de servidores
- Amenaza 4: Incendio

Las variables claves o problemas claves. La parte final del análisis realizado consiste en identificar los problemas claves del sistema; que serían aquellos que presentan mayores niveles de motricidad y dependencia y se encuentran ubicados en las zonas de poder y conflicto.

Para el caso en estudio se tiene que las variables ubicadas en dichas zonas, es decir de poder es la identificada con el número: 25 y es:

- Amenaza 25: Alteración malintencionada del software de aplicación, mediante la inclusión dentro del código de programas que se instalan como: virus, caballos de Troya u otras amenazas.

Mientras que las que se ubicaron en la zona de conflicto como la 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,26 y 27 tenemos las siguientes:

- Amenaza 5: Acceso físico

- Amenaza 6: El sistema de ficheros
- Amenaza 7: Permitir montar y desmontar sistemas de ficheros a los usuarios
- Amenaza 8: Los bits setuid y setgid
- Amenaza 11: FTP (File Transfer Protocol): puerto TCP 21
- Amenaza 12: Telnet: puerto TCP 23
- Amenaza 13: SMTP (Simple Mail Transfer Protocol): puerto TCP 25
- Amenaza 14:Finger: puerto TCP 79
- Amenaza 15: rexec: puerto TCP 512
- Amenaza 16: rlogin: puerto TCP 513 y rsh: puerto TCP 514
- Amenaza 17: NFS (Network File System): puerto TCP 2049
- Amenaza 18: RPC (Sun Remote Procedure Call) : Puerto UDP 111
- Amenaza 19: SNMP (Simple Network Management Protocol): puerto UDP 161
- Amenaza 20: Syslog: Puerto UDP 514
- Amenaza 21: Identificación de direcciones IP -Servidores UIS
- Amenaza 22: Exploración de puertos al Firewall de la UIS y routers ETB y TELECOM
- Amenaza 23: Violación del Websense
- Amenaza 24: Violación de los servidores de correo de la UIS.
- Amenaza 26: Divulgación, modificación, interceptación, pérdida total o parcial de los datos.
- Amenaza 27: Atacante interno. Sistema de autenticación de UNIX, revelado de contraseñas.

Valoración del Riesgo. La metodología prospectiva anterior permitió valorar el nivel de riesgo y costo asociado de cada una de las amenazas así:

Amenaza 1. Fluctuaciones en la tensión o frecuencia en el suministro de energía eléctrica como:

- Corte total de energía
- Baja tensión
- Variaciones en la frecuencia
- Picos de alta tensión
- Sobretensión
- Caídas de Tensión

Nivel de Riesgo: Bajo.

Costo Asociado: Las variaciones y cortes en el fluido eléctrico pueden afectar no sólo a Pelicano sino también a cualquier otro servidor en su: memoria, fuentes, tarjetas de circuitos, lo mismo que las lecturas y grabaciones en los discos duros, a pesar de disponer de UPS con ½ hora de soporte ante fallo de energía, siendo la pérdida de información, la peor de las consecuencias. Los daños por hardware pueden producirse y acarrear cuantiosas pérdidas, pero estas serían cuantificables. La consecuencia más delicada o crítica derivada de esta amenaza sería el no poder disponer del servidor en el momento que se necesite, retrasando

el cumplimiento de las funciones tanto académicas como administrativas asignadas.

Amenaza 2. Daño o falla en alguno de los componentes hardware del equipo (discos duros, memoria, procesadores, tarjetas de circuitos, fuente, etc.

Nivel de Riesgo: Bajo

Costo Asociado: Los daños de hardware en Pelicano o cualquier otro equipo de la sala ocasionaría n problemas de disponibilidad en el servidor durante el tiempo que se demore la corrección del problema, afectando el normal desempeño tanto de las labores académicas como administrativas que dependen del servidor. De acuerdo a la parte dañada dependerá la gravedad de las consecuencias, de dañarse un disco duro, el principal problema sería la recuperación de la información almacenada. Si la falla es en la memoria, la fuente, el procesador, u otra, el retraso dependería principalmente en el tiempo que lleve reemplazar la pieza dañada y poner nuevamente a funcionar el servidor.

Amenaza 3. Elevada temperatura en la sala de servidores

Nivel de riesgo: Bajo

Costo Asociado: Los aumentos de temperatura en la sala de servidores pueden ocasionar bloqueos en los equipos o deficiencia en el rendimiento de los componentes hardware de los mismos.

Amenaza 4. Incendio

Nivel de Riesgo: Bajo

Costo Asociado: La instalación del aire acondicionado puede ser una fuente de incendios, como también las acometidas eléctricas defectuosas. Un incendio provocaría la pérdida total o parcial de las instalaciones físicas y de la información en caso de no tener respaldos de seguridad almacenados en otras localizaciones.

Amenaza 5. Acceso físico

Nivel de Riesgo: Medio

Costo Asociado: La falta de controles en el acceso físico del personal a la sala de servidores, facilitaría el ingreso de comida, bebidas o de personal ajeno a las funciones propias de esta sala. Esto también podría conducir al robo o al extravío de elementos físicos, o de información (informes, listados, copias de seguridad, etc.). Otro hecho que pudiera suceder a la UIS como universidad pública que es, la pluralidad de corrientes de pensamiento que recorren sus claustros, donde se

reflejan las problemáticas sociales tanto del país como del mundo, no estaría exenta de actos de terrorismo como la colocación de artefactos explosivos en las sala de servidores. Así mismo, la información contenida en los diferentes listados o la almacenada en las copias de seguridad puede ser leída o destruida por cualquier persona sino se tienen los debidos controles en la sala.

Sistema Operativo. Pelícano cuenta con el Sistema Operativo IRIX64 versión 6.5.12 propiedad de Silicon Graphics. En la actualidad UNIX puede considerarse como el sistema operativo de propósito general más fiable del mercado; desde los clones habituales (Solares, HP-UX, IRIX) hasta los Trusted Unix[18], pasando por los sistemas gratuitos (Linux, FreeBSD), cualquier entorno Unix puede ofrecer los mecanismos de seguridad suficientes para satisfacer las necesidades de la mayoría de instituciones. Los sistemas operativos Unix habituales, como Solaris o Linux, son bastantes inseguros si se instalan por defecto, requieren de una mínima puesta a punto, en cuanto a seguridad, antes de ponerlos a trabajar con unas mínimas garantías de fiabilidad. Al efectuarse esta puesta a punto suelen tener una seguridad aceptable en redes de propósito general. El problema es que generalmente se pone a trabajar a Unix tal y como se instala por defecto, lo que convierte a cualquier sistema operativo, Unix o no, en un agujero de seguridad; cuentas sin password o con passwords por defecto, servicios abiertos, sistemas de ficheros compartidos, entre otros.

En este apartado se analizan algunas de las vulnerabilidades conocidas en el sistema operativo Unix y se realiza la exploración del servidor Pelicano a través de la utilización de herramientas software tipo Network Scanner, que permiten evaluar la seguridad de la red, realizando exploración de puertos y de seguridad de la máquina o segmento de red indicado. Este tipo de herramientas se encuentran disponibles en Internet, y tienen como objetivo principal permitirle al administrador de red, auditar la seguridad de su red de manera rápida y fácil, generando reportes en los que se exponen las falencias encontradas y se sugieren medidas de contención para solucionar dichas debilidades. Cabe resaltar, que al estar disponibles en Internet pueden ser usadas con doble faz: por administradores de red o por posibles hackers, por ello la constante auditoría de la seguridad de la red es un punto importante para ser tenido en cuenta por todo administrador de la seguridad en redes.

Concretamente la exploración de vulnerabilidades de Pelícano se llevó a cabo haciendo uso de tres herramientas: GFI LANguard Network Security

[18] Unix Seguros (Trusted Unix): son sistemas operatives con excelentes sistemas de control, evaluados por la National Security Agency (NSA) estadounidense y clasificados en niveles seguros (B o A). Entre estos Unix seguros podemos encontrar AT&T System V/MLS y OSF/1, Trusted Xenix8 y XTS-300 STOP 4.1, considerados los sistemas operativos más seguros del mundo (según la NSA). La gran mayoría de Unices (Solares, AIX) están clasificados como C2, y algunos otros, como Linux, se consideran sistemas C2 de facto: al no tener una empresa que pague el proceso de evaluación de la NSA no están catalogados, aunque puedan implementar todos los mecanismos de los sistemas C2.

Scanner(LNSS)[19], NmapWin[20], y Shadow Security Scanner (SSS)[21]. Como producto de estas exploraciones, se generaron reportes en los que se relacionan las falencias encontradas y se proponen medidas de contención. De acuerdo a los resultados obtenidos, se procedió a analizar cada vulnerabilidad encontrada, el nivel de riesgo de la amenaza y las medidas de contención disponible para controlarlas.

Amenazas encontradas en el Sistema Operativo de Pelícano y Medidas de Contención.

Amenaza 6: El Sistema de Ficheros. La filosofía de diseño de Unix en la cual todo son archivos: la memoria física del equipo, los discos, las impresoras, el teclado, los terminales, la unidad de cinta, etc, es uno de los factores que más éxito y potencia ha proporcionado a este sistema operativo, pero a la vez le han originado grandes peligros.

Nivel de Riesgo: Medio

Costo Asociado: Los permisos otorgados a un archivo determinan quién puede leer, modificar o ejecutar los ficheros almacenados en el sistema Unix. Un error en un permiso puede causar que un usuario pueda modificar todo un disco duro, ejecutar comandos a los que no debería tener derechos o leer archivos e información a la que no debiera tener acceso. Por tal motivo la correcta utilización de los permisos, atributos y otros controles sobre los ficheros son de vital importancia para la seguridad del sistema.

Amenaza 7. Permitir montar y desmontar sistemas de ficheros a los usuarios (generalmente unidades de disquete o CD-ROM), también puede convertirse en una amenaza de seguridad sino es implantada correctamente.

Nivel de Riesgo: Medio.

Costo Asociado: El archivo /etc/fstab (su nombre depende del clon de Unix), enseña qué sistemas de ficheros se montan cuando la máquina arranca y bajo qué nombre de directorio. Dicho montaje se realiza con ciertas opciones tomadas por defecto; como son: rw (se permite tanto la lectura como la escritura), suid (se permite la existencia de ficheros setuidados), dev (se permite la existencia de dispositivos), exec (se permite la ejecución de binarios), auto (el sistema se monta automáticamente al arrancar o al utilizar mount-a), nouser (sólo puede ser

[19]GFI.LANguard Network Security Scanner (LNSS). Available from Internet: <http://www.gfisoftware.com/lannetscan/>
[20] Insecure.org. NmapWin. Available from Internet: <http://www.insecure.org/nmap/index.html>
[21] Safety-Lab. Shadow Security Scanner (SSS). Available from Intemet: <http://www.safety-lab.com/en/products/1.htm>

montado por el root) y async (la entrada/salida sobre el dispositivo se realiza de forma asíncrona). Estas son las opciones más lógicas para los sistemas de ficheros normales, pero no para los que pueden montar los usuarios. Si se les deja a los usuarios sin privilegios, montar y desmontar su dispositivo con las opciones por defecto, es posible que accesen directamente al hardware, por ejemplo, para destruir completamente los discos duros o bloquear la máquina; conseguir privilegios de administrador con la ejecución de un shell o ejecutar un programa almacenado en el dispositivo que él montó.

Amenaza 8. Los bits de setuid y setgid proporcionan a Unix una gran flexibilidad, pero constituyen al mismo tiempo la mayor fuente de ataques internos al sistema (entendiendo por ataques internos aquellos realizados por un usuario autorizado o no, desde la propia máquina, generalmente con el objetivo de aumentar su nivel de privilegio en la misma). La consecuencia de activar el bit setuid sobre un fichero implica que todo aquel que ejecute el archivo va a tener durante su ejecución los mismos privilegios que quién lo creó; es decir, si el administrador crea un fichero y lo setuida, todo aquel usuario que lo ejecuta va a disponer, hasta que el programa finalice, de un nivel de privilegio total en el sistema. El archivo se ve de la siguiente manera:

```
>ls –l  /bin/passwd
>-rwsr-xr-x   1 root   sys 30552  Jun 25 2005 /bin/passwd
```

Todo lo expresado con relación al bit setuid es aplicable al bit setgid pero a nivel de grupo del fichero en lugar de propietario: en lugar de trabajar con el EUID del propietario, todo usuario que ejecute un programa setgidado tendrá los privilegios del grupo al que pertenece el archivo. Si el fichero es un directorio y no un archivo plano, el bit setgid afecta a los ficheros y subdirectorios que se creen en él: estos tendrán como grupo propietario al mismo que el directorio setgidado, siempre que el proceso que los cree pertenezca a dicho grupo. El archivo se observa de la siguiente manera:

```
> ls –l /bin/passwd
> -rwsr-sr-x   1 root   sys 30552  Jun 25 2005  /bin/passwd
```

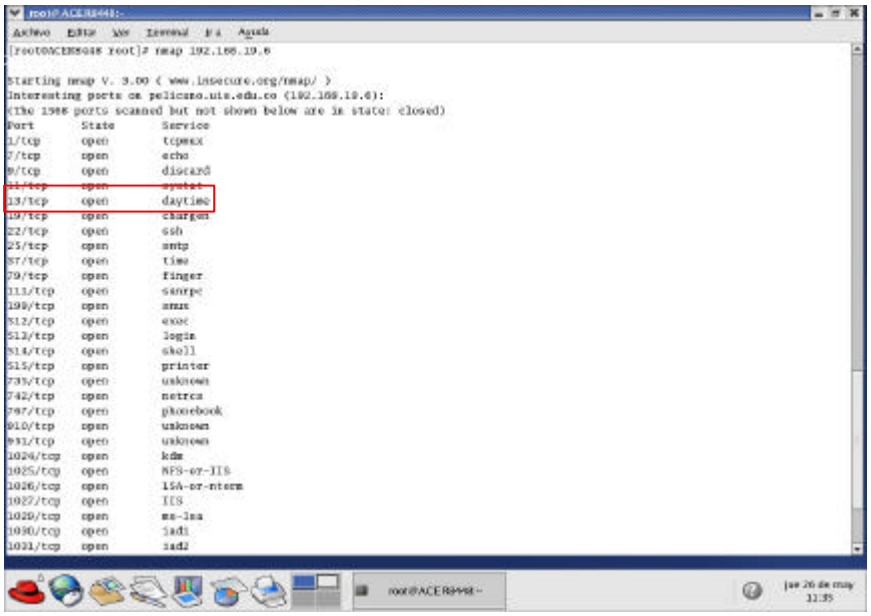
Nivel de Riesgo: Medio

Costo Asociado: Los sistemas Unix tienen cierto número de ejecutables setuidados y/o setgidados. Cada uno de ellos se ejecuta con los privilegios de quien lo creó, lo que directamente implica que cualquier usuario tiene la capacidad de lanzar tareas que escapen total o parcialmente al control del sistema operativo: se ejecutan en modo privilegiado si es el administrador quien creó los ejecutables. Evidentemente, estas tareas han de estar controladas de forma exhaustiva, ya que si una de ellas se comporta en forma anormal (un simple core dump) puede causar daños irreparables al sistema. Algunos de los archivos setuidados son estrictamente necesarios en Unix, como es el caso de /bin/passwd, la orden para que los usuarios puedan cambiar su contraseña de entrada al sistema, una de sus

funciones consiste en modificar el fichero de claves (/etc/passwd o /etc/shadow). Un usuario normal no tiene el nivel de privilegio necesario para hacer esto (es posible que ni siquiera pueda leer el fichero de claves), por lo que frente a este problema parece imprescindible el bit de setuid en el archivo /bin/passwd.

Debilidades de los Servicios Disponibles en el Servidor Pelícano.

Figura 23. Amenaza 9: Daytime: Time of Day, Puerto TCP 13



Fuente: Autor del proyecto

Nivel de Riesgo: Medio.

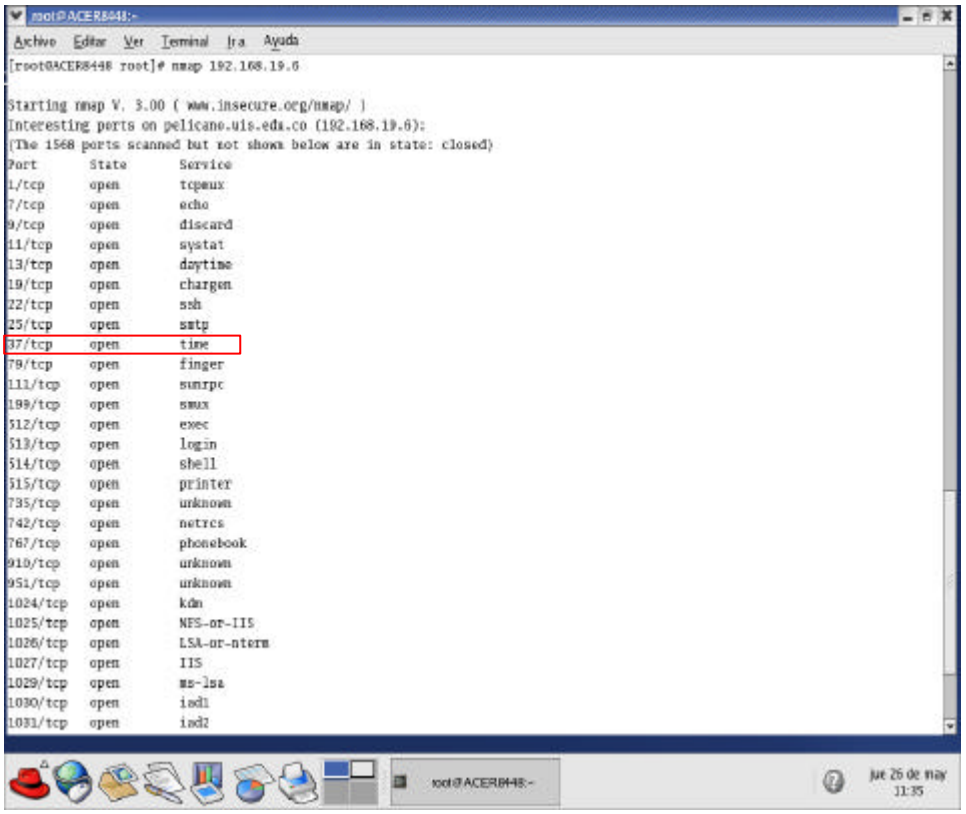
Costo Asociado: Daytime es un servicio interno de inetd (debido a que no hay un programa externo que lo sirva, por lo tanto inetd se encarga de ello); al recibir una conexión a este puerto, el sistema muestra la fecha y la hora:

>telnet pelicano **daytime**
Trying 192.168.19.6…
Connected to pelicano.uis.edu.co.
Escape character is '^]'.
Mon Jun 4 14:30:23:34 2004
Connection closed by foreign host.

A simple vista este servicio parece no representar peligro para la integridad del sistema, pero una norma de seguridad dice: se debe ofrecer sólo los servicios estrictamente necesarios para el correcto funcionamiento de nuestras máquinas.

Como daytime no es un servicio básico, se aconseja cerrarlo; porque la información que proporciona aunque escasa, puede ser empleada por un atacante en el sentido de que le informa el estado del reloj del sistema, brindándole una idea de la ubicación geográfica del equipo.

Figura 24. Amenaza 10: Time: puerto TCP 37



Fuente: Autor del proyecto.

Nivel de Riesgo: Medio.

Costo Asociado: Muestra la fecha y hora del equipo, pero en un formato que no entendible para las personas.

>telnet pelicano **time**
Trying 192.168.19.6…
Connected to pelicano.uis.edu.co.
Escape character is '^]'.
ÂÖ<Connection closed by foreign host.

Este servicio es más útil que daytime: una persona no entiende la información mostrada por time, pero sí una máquina Unix. Se emplea time en un servidor para que las estaciones cliente puedan sincronizar sus relojes con él con comandos como netdate o rdate. Se recomienda cerrar este servicio, aunque existen situaciones en las que un administrador prefiere ofrecer time en varias máquinas que ofrecer daytime.

Amenaza 11. FTP (File Transfer Protocol): puerto TCP 21.

Nivel de Riesgo: Medio

Costo Asociado: FTP es un protocolo de transferencia de ficheros entre sistemas. Permite conectar un equipo cliente a un servidor con el fin de descargar o enviar ficheros.

Uno de los principales inconvenientes de FTP es su diseño, debido a que está orientado a ofrecer máxima velocidad en la conexión, pero no para ofrecer seguridad; ya que todo intercambio de información que se efectúe, desde el login y el password del usuario en el servidor hasta la transferencia de cualquier archivo se realiza en texto claro, haciendo posible que un atacante pueda capturar tráfico usando un sniffer y conseguir un acceso válido al servidor. Otra amenaza a la privacidad de los datos puede surgir si el atacante captura y reproduce los archivos transferidos.

Amenaza 12: Telnet: puerto TCP 23

Nivel de Riesgo: Medio.

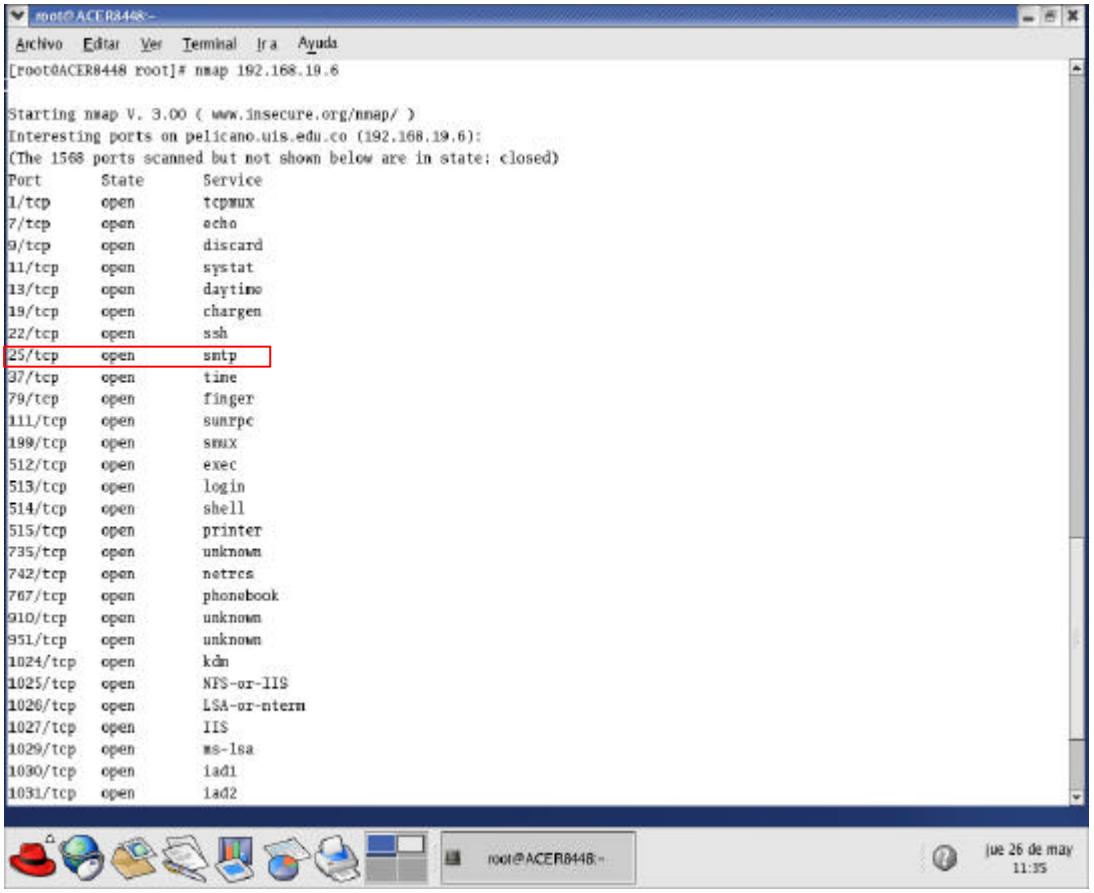
Costo Asociado: El servicio Telnet permite utilizar una máquina como terminal virtual de otra a través de la red, de manera que se establece un canal virtual de comunicaciones parecido pero mucho más inseguro a utilizar una terminal físicamente conectada al servidor. Telnet accede remotamente en modo texto a un equipo en principio potente, permitiendo aprovechar su fortaleza de cálculo sin necesidad de desplazamiento hasta la ubicación de ese servidor, trabajando desde nuestro propio equipo. La versión Unix de telnet está implementada con los programas cliente telnet y el servidor telnetd.

A pesar de ser Telnet un servicio muy útil, no utiliza ningún tipo de cifrado, transmitiendo todo el tráfico entre equipos en texto claro, facilitando a un atacante con un analizador de red (o un sniffer) capturar el login y el password utilizado en la conexión; permitiendo un acceso total a la máquina destino bajo nuestra identidad.

Los demonios telnetd han presentado frecuentemente problemas de programación; ya que cualquier versión de este demonio que no esté actualizada

es una potencial fuente de problemas, por lo que se recomienda conseguir la última versión de telnetd para el Unix particular, principalmente para versiones anteriores a 1997. También pueden afectar este servicio amenazas como es el hecho de que un atacante consiga recuperar una sesión que no ha sido cerrada correctamente, el uso de telnet para determinar qué puertos de un host están abiertos, o la utilización del servicio telnet para averiguar el clon de Unix concreto (versión de kernel incluida) que un servidor utiliza, han hecho famosa la inseguridad de este servicio.

Figura 25. Amenaza 13: SMTP (Simple Mail Transfer Protocol): puerto TCP 25



Fuente: Autor del proyecto.

Nivel de Riesgo: Medio

Costo Asociado: El servicio SMTP es empleado para transferir correo electrónico entre equipos remotos. Este servicio suele ser efectuado por un demonio denominado sendmail, el cual ha sido fuente de numerosos huecos de seguridad en los sistemas Unix, dentro de las cuales se resaltan debilidades como:

- Facilitar mediante el envío de un correo electrónico formateado de manera especial, que los intrusos informáticos puedan hacerse con el control del servidor de correo. Vulnerabilidad muy delicada porque el atacante no necesita ningún conocimiento específico sobre su objetivo.

- Permitir que un atacante de acuerdo a su habilidad, acceda remotamente como root al sistema objetivo.

- Facilitar a una dirección de correo errónea ejecutar un buffer overflow sobre el servidor.

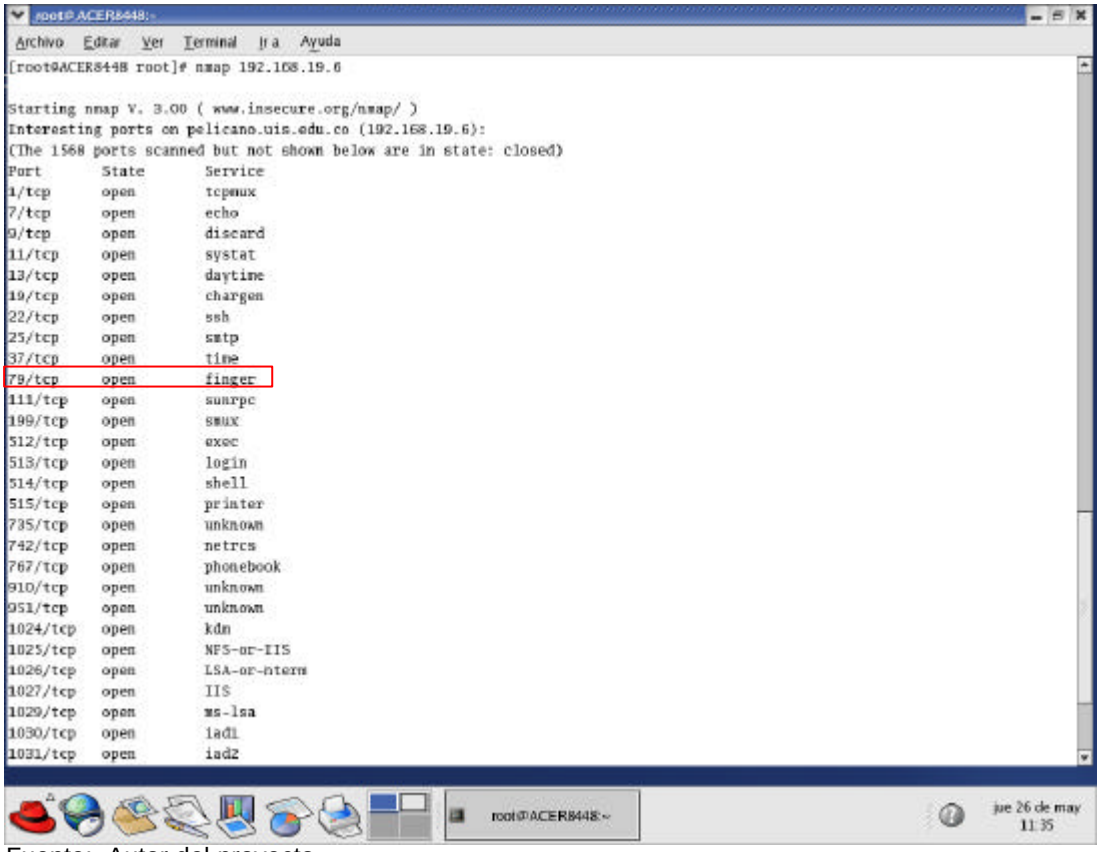
Sendmail presenta problemas debido a su diseño complicado, su programación en un solo bloque, corre como superusuario y acepta conexiones desde cualquier computador en internet, además posee una gran variedad de comandos, factores que no hacen extraño la presencia de agujeros de seguridad en su código. Ninguna versión de sendmail anteriores a la 8.11.6 es recomendable debido a fallas graves de seguridad. El fichero de configuración principal de sendmail es /etc/sendmail.cf y los comandos VRFY y EXPN también presentan fallos de seguridad por lo tanto deben ser deshabilitados. VRFY permite a alguien hacer telnet al servidor de sendmail con el fin de averiguar si es una dirección válida, facilitando ataques de tipo spam. Además, muchos ataques informáticos a redes comienzan averiguando un nombre de cuenta válida en una máquina.

Ejemplo:

```
>telnet localhost 25
Trying 127.0.0.1…
Connected to localhost.
Escape character is '^]'.
220 pelicano.uis.edu.co ESMTP Sendmail SGI-8.9.3; Mon, 21 Jun 2004
15:33:25-0400 (EDT)
vrfy root
250 Super-User<root@pelicano.uis.edu.co>
vrfy poncho
550 pepito...User unknown
quit
221 pelicano.uis.edu.co closing connection
Connection closed by foreign host.
```

Otro comando de cuidado es **EXPN,** ya que permite hacer telnet al servidor de sendmail y proporcionar un alias. Este comando proporciona la lista de todas las direcciones de correo que pertenecen al alias y se hace peligroso, debido a que muchas máquinas tienen listas de usuarios, que al ser expandidas permiten obtener los nombres de muchos usuarios, situación que puede ser aprovechada por un atacante.

Figura 26. Amenaza 14: Finger: Puerto TCP 79



Fuente: Autor del proyecto.

Nivel de Riesgo: Medio.

Costo Asociado: Finger es un protocolo que proporciona información muy completa de los usuarios de una máquina, estén o no conectados en el momento de acceder al servicio. Finger puede utilizarse de dos formas: dándole como argumento el nombre de máquina precedido del símbolo "@" o el nombre de un usuario seguido de "@".

- Condor> finger @pelicano

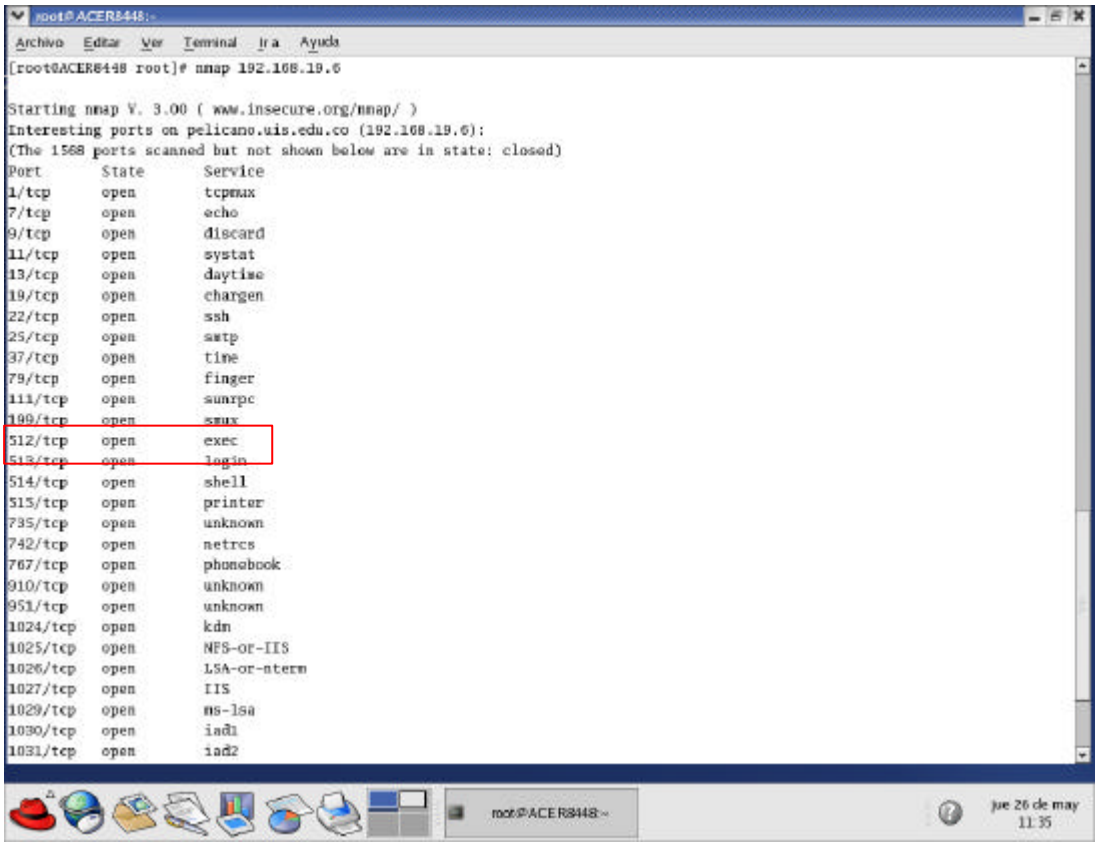
Finger mostrará datos generales de los usuarios que se encuentren conectados en ese momento a la máquina: nombre de usuario, nombre completo, tiempo de login, número telefónico de la oficina (asumiendo que esta información está almacenada en el archivo /etc/passwd).

- Condor> finger usuariox@pelicano

Finger busca en etc/passwd e informa en detalle acerca del usuario o los usuarios cuyos apellidos, nombres o username coincidan con el parámetro especificado, estén o no conectados.

La información suministrada por finger es de mucha utilidad para un atacante (nombres de usuario, hábitos de conexión, cuentas inactivas, directorio HOME del usuario, número telefónico de la oficina, entre otros) y puede ser usada como base para un ataque de ingeniería social contra los usuarios o contra el propio administrador del sistema.

Figura 27. Amenaza 15: rexec: Puerto TCP 512



Fuente: Autor del proyecto.

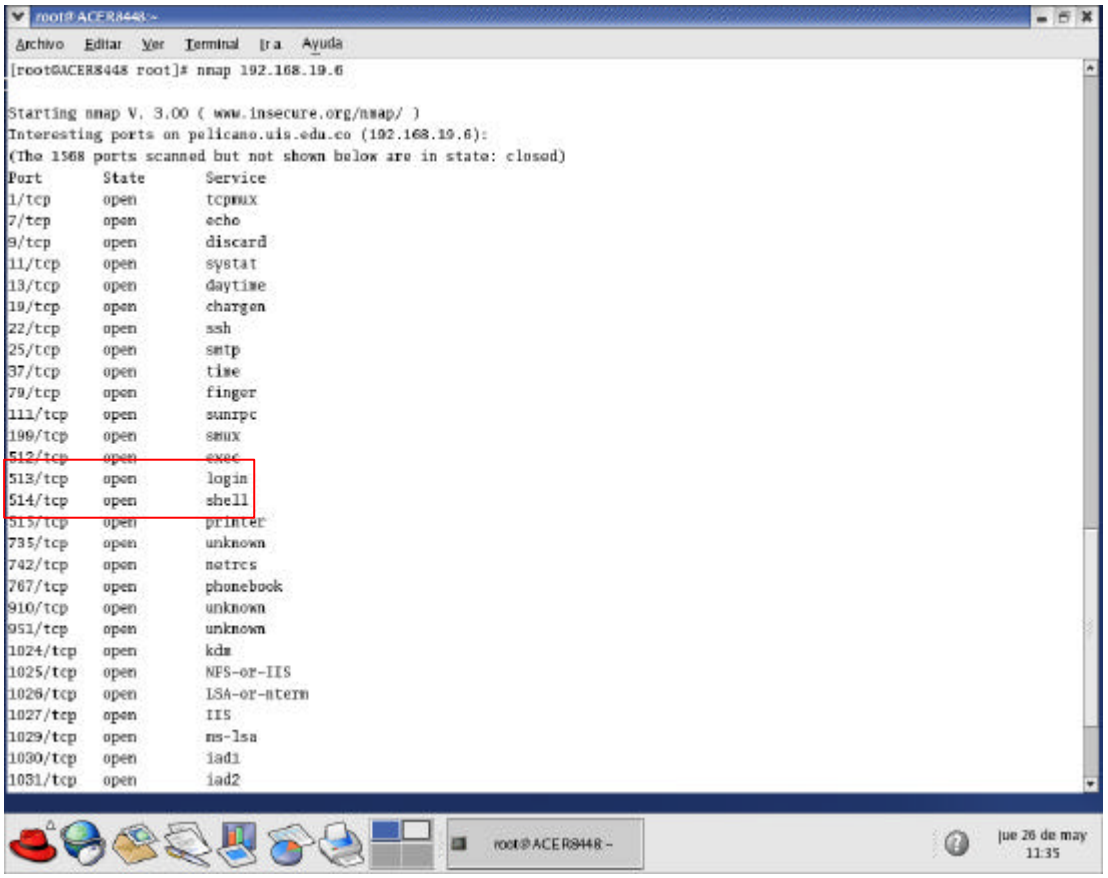
Nivel de Riesgo: Medio.

Costo Asociado: Unix posee los servicios r * que son herramientas con una parte cliente y una servidora que se encargan de la conexión remota entre máquinas, especialmente para servicios de terminal remota y también transferencia de ficheros. Las componentes clientes son rsh, rlogin y rcp, mientras que las servidoras son demonios como rexecd, rshd o rlogind, los cuales pueden presentar inconvenientes tales como: rexecd. Es un demonio de ejecución remota /usr/sbin/rexecd que le permite al usuario la ejecución de comandos sobre otros equipos sin necesidad de loguearse en ellos. El problema surge cuando el cliente abre una conexión y transmite un mensaje que especifique tanto el username, el

password y el nombre del comando a ejecutar. Como rexecd necesita que el password sea transmitido por la red, este puede ser capturado por un sniffer como también puede ocurrir con un telnet.

Es conveniente resaltar que rexecd emite mensajes de error diferentes para username inválidos y password errados diferentes a telnet. Si el username resulta inválido, rexecd retorna el mensaje de error “login incorrecto”. Si el username es correcto y el password es erróneo devuelve un mensaje de error “password incorrecto”. Esta situación pudiera provocar que un atacante se aprovechara de rexecd para adivinar passwords partiendo de usuarios válidos.

Figura 28. Amenaza 16: rlogin: Puerto TCP 513 y rsh: Puerto TCP 514



Fuente: Autor del proyecto.

Nivel de Riesgo: Medio.

Costo Asociado: rlogin se emplea como terminal virtual de un sistema Unix, de manera muy similar a telnet; donde rlogin es el programa cliente y rlogind es el servidor. Así mismo, rsh es utilizado para ejecutar comandos en una máquina

remota sin necesidad de acceder a ella; rsh es el cliente y rshd es el servidor. Tanto rlogin como rsh están diseñados para comunicación sólo entre sistemas Unix Berkeley. Los usuarios que deseen comunicarse entre Unix y TOPS, VMS, u otra clase de sistemas deben usar el protocolo telnet, no el protocolo rlogin.

Los servicios r* evitan el tránsito de contraseñas por la red, y fue conseguido por los diseñadores del sistema de red de Unix BSD mediante la idea de "máquinas fiables" y "usuarios fiables" donde cualquier usuario, puede hacer uso de los recursos de una máquina remota sin necesidad de una clave si su conexión proviene de una máquina fiable o si su nombre de usuario es fiable.
Es posible considerar una máquina fiable de dos formas:

1. Si su nombre (el de la máquina) se encuentra en el directorio /etc/hosts.equiv.

2. Si su nombre (el de la máquina) se encuentra en un fichero denominado .rhosts situado en el $HOME del usuario.

En el primer caso, cualquier usuario (excepto el root) del sistema remoto (y fiable) puede acceder al equipo bajo el mismo login que tiene en el primero, sin necesidad de claves. En el segundo caso, empleando los ficheros .rhosts, cualquier usuario del sistema remoto podrá conectar al nuestro pero sólo bajo el nombre de usuario en cuyo $HOME se encuentra el archivo.

El concepto de usuarios fiables es el mismo que el asociado al de máquinas fiables, pero aplicado a nombres de usuario en lugar de nombres de máquina. Los nombres de usuario pueden indicarsen tanto en /etc/hosts.equiv como en los archivos .rhosts; no obstante, la primera opción no es apropiada debido a que permite al usuario fiable del sistema remoto acceder sin contraseña a cualquier cuenta de nuestra máquina. Por lo tanto para crear usuarios fiables de sistemas remotos, es necesario hacerlo en los archivos .rhosts.

Las relaciones de confianza entre equipos Unix suelen ser muy útiles y cómodas, pero paralelamente son muy peligrosas: ya que si se confía plenamente en sistemas remotos, de llegar a comprometerse su seguridad, también se afectaría la seguridad de otros equipos. Las máquinas fiables se deben reducir a equipos de la misma organización, y administrados por la misma persona; también, es necesario tener presente que al tener habilitados los servicios r* cualquier usuario puede establecer relaciones de confianza. Así mismo, es necesario chequear los directorios $HOME en busca de ficheros .rhosts; y seguir la estrategia de muchos administradores que prefieren no complicarse buscando estos ficheros, y configurar sus sistemas para que en cada $HOME exista un fichero con este nombre, propiedad de root y con modo 000, evitando de esta de esta forma que los usuarios no tengan ocasión de otorgar confianza a sistemas remotos.

Las relaciones de confianza son transitivas, lo cual quiere decir que si una máquina confía en otra, lo hace también en todas en las que confía ella. Así, se crean anillos de confianza entre máquinas. El mecanismo de máquinas fiables usa direccionamiento IP para autenticación por lo cual es vulnerable a ataques por IP

spoofing y ataques DNS. Si un intruso consigue hacer pasar su equipo por uno de los confiables, automáticamente ha conseguido acceso (casi ilimitado) al resto de las máquinas.

Amenaza 17. NFS (Network File System): Puerto TCP 2049

Nivel de Riesgo: Medio.

Costo Asociado: NFS es uno de los servicios RPC[22] más ampliamente usados. NFS se encarga que usuarios de una red puedan acceder a archivos almacenados en un servidor. Dicho servicio presenta implicaciones de seguridad tanto para el servidor NFS como para el cliente NFS, como las siguientes:

- Acceso Cliente: NFS debe ser configurado para que sólo determinados clientes o hosts en la red puedan montar sistemas de archivos en el servidor. Varias versiones de UNIX, como IRIX de SGI usan el archivo /etc/exports para designar cuáles clientes pueden montar sistemas de archivos y los permisos concedidos.

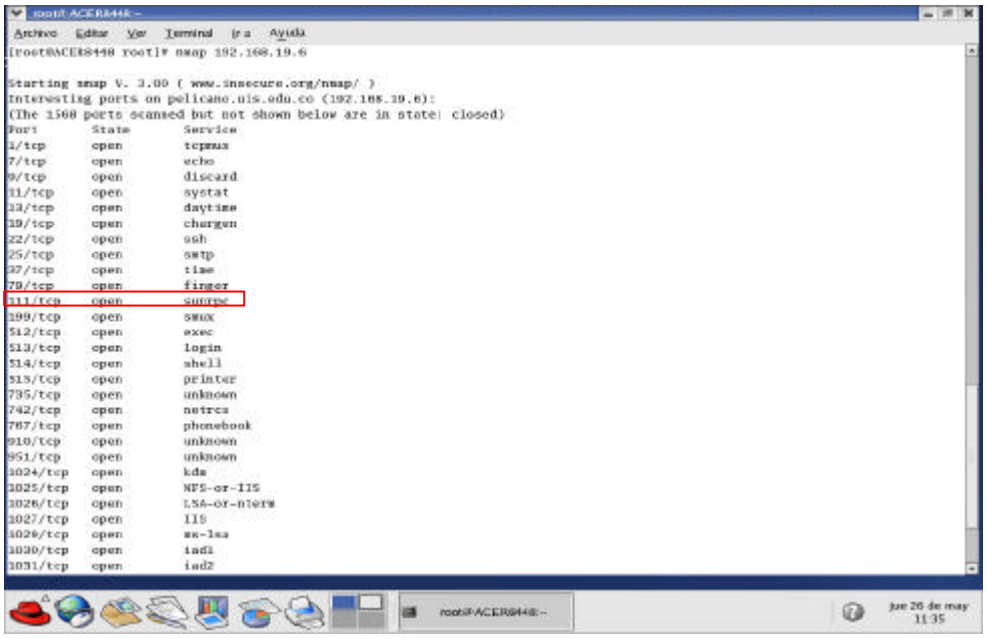
- Autenticación de Usuario: NFS debe ser configurado para que los usuarios puedan acceder y modificar sólo los archivos a los cuales se les ha otorgado el privilegio de hacerlo.

Eavesdropping y spoofing de datos. NFS no protege la información de la red de este tipo de ataques, ya que el sistema primario que NFS usa para autenticación de servidores está basado en direcciones IP y hostnames. Además como los paquetes NFS no viajan encriptados, puede suceder que un atacante logre engañar (spoof) un cliente NFS haciéndose pasar como un servidor NFS o cambiar los datos que viajan entre el servidor y el cliente. De este modo el intruso puede forzar a una máquina cliente a correr cualquier ejecutable montado en un NFS. Lo cual le daría al atacante el completo control sobre una máquina NFS cliente.

[22] RPC Remote Procedure Call. Mecanismo que le permite a un programa que está corriendo en un computador ejecutar una función que está corriendo en otro computador. Facilita la creación de redes basadas en programas cliente/servidor: los clientes y el servidor se comunican entre ellos usando RPC

Puertos UDP abiertos.

Figura 29. Amenaza 18: RPC (SUN Remote Procedure Call) puerto UDP 111



Fuente: Autor del proyecto.

Nivel de Riesgo: Medio.

Costo Asociado: RPC es otra forma de ofrecer servicios al igual que inetd o los demonios independientes lanzados al arrancar el sistema; original de SUN Microsystems pero en la actualidad está implementado también por OSF (Open Software Foundation) en su DCE (Distributed Computing Environment) y por OMG (Open Management Group) en CORBA (Common Object Request Broker Architecture). El funcionamiento básico RPC radica en la existencia de un programa denominado portmap, rpcbind, rpc.pormap (su nombre depende del clon de Unix) que los servidores RPC utilizan para registrarse, de tal forma que cuando un cliente desea utilizar esos servicios, en lugar de conectar a un puerto determinado donde se encuentre el servicio lo hace al puerto del portmapper, que le facilitará la ubicación exacta del servicio solicitado. Portmapper es aprovechado para asignar dinámicamente los puertos TCP y UDP usados para llamados de procedimiento remoto, es muy parecido al demonio inetd, en el sentido de que media en las comunicaciones entre clientes y servidores de red, los cuales podrían tener problemas de seguridad.

El portmapper estándar de UNIX, delega el manejo de la seguridad a los servidores, permitiendo además que cualquier cliente de la red se comunique con cualquier servidor RPC, resultando los mecanismos RPC generalmente muy

complejos, y difíciles para garantizar la seguridad en ellos. Algunas de las vulnerabilidades detectadas en los servicios RPC se listan a continuación:

- Rpc.statd. Demonio de estado RPC NFS, componente de la arquitectura Network File System (NFS). Es parte del paquete de utilidades NFS distribuido en Linux y es empleado para comunicar información del estado a otros servicios o hosts, pero presenta también varias debilidades asociadas. Dentro de las vulnerabilidades encontradas se tiene la del formato string en el llamado a la función a la función syslog(), en la que un usuario remoto malicioso puede ejecutar código como root. Otra debilidad puede ser explotada por un atacante para crear o modificar archivos con privilegios de root. La versión de statd contenida en muchas implementaciones de UNIX contiene una condición buffer overflow. El atacante que intente explotar satisfactoriamente esta vulnerabilidad podrá ganar privilegios de root sobre el host objetivo. Una posible solución para corregir estos problemas es actualizar la versión actual de statd.

- FAM. Algunas versiones de este servicio son vulnerables, corren arbitrariamente comandos como root.

- Valid. Un atacante puede usar este servicio para hacer spoofing a mensajes de consola.

Amenaza 19: SNMP (Simple Network Management Protocol) puerto UDP 161

Nivel de Riesgo: Medio.

Costo Asociado: El protocolo SNMP se diseñó para permitir la administración remota de los dispositivos sobre la red, por lo tanto permite a los administradores de sistemas y de redes supervisar y configurar remotamente dispositivos sobre la red (switches y routers, entre otros). Para el protocolo SNMP la red está compuesta por un grupo de elementos básicos: Administradores o gestores ubicados en el/los equipo/s de gestión de red y Agentes, elementos pasivos ubicados en los nodos (host, routers, modems, multiplexores, etc.) a ser gestionados, siendo estos últimos los que envían información a los primeros, relacionada con los elementos gestionados, por iniciativa propia o al ser interrogados (polling) de manera secuencial, soportada en los parámetros contenidos en sus MIB (Management Information Base).

El protocolo SNMP muestra dos tipos de mensajes de administración:

- Mensajes para cambiar el estado de un dispositivo en la red.
- Mensajes que supervisan el estado actual de la red.

Estos mensajes cuidadosamente construidos por el SNMP pueden ser de gran valor para los atacantes porque pueden conocer la estructura interna de la red, efectuar un ataque de negación de servicio o cambiar la configuración de la red. Aunque algunos sistemas SNMP incluyen mejoras de seguridad basadas en contraseñas, para lo cual emplean el nombre de la comunidad como un password, el cual es transmitido en texto claro permitiendo que el nombre de la comunidad quede expuesto.

Cada administrador de la red debe sopesar el valor de cada servicio particular del SNMP contra el riesgo que supone el protocolo.

Amenaza 20: Syslog Puerto UDP 514

Nivel de Riesgo: Medio.

Costo Asociado: El demonio syslog (Syslog Daemon) se activa automáticamente al arrancar el sistema Unix, se encarga de guardar informes sobre el funcionamiento de la máquina, además recibe mensajes de las diferentes partes del sistema (núcleo, programas, dispositivos) y los envía y/o almacena en diferentes localizaciones, tanto locales como remotas, acorde a criterios definidos en el fichero de configuración /etc/syslog.conf, el cual especifica las reglas a seguir para gestionar el almacenamiento de los mensajes del sistema. Syslog puede recibir mensajes de log desde tres fuentes y estas son:

- /dev/klog: dispositivo especial, usado para leer mensajes generados por el kernel.
- /dev/log: Unix domain socket, usado para leer mensajes generados por procesos corriendo sobre la máquina local.
- UDP puerto 514: Internet domain socket, usado para leer mensajes generados sobre la red de área local desde otras máquinas.

Syslog, por defecto, puede aceptar mensajes de log de hosts arbitrariamente enviados al puerto local del UDP del syslog. Esta situación abre la posibilidad de un ataque de negación de servicio, en caso de que el puerto se inunde con mensajes más rápidos de los que el demonio del syslog pueda procesar, también mensajes fraudulentos pueden ser enviados deliberadamente al puerto, con el objetivo de obtener privilegios en el sistema y llegar a ejecutar código como root.

Amenaza 21: Identificación de direcciones IP - Servidores UIS.

Empleando la herramienta Nmap se efectuaron las siguientes pruebas que dieron como respuesta la identificación de las IPs y nombres de importantes servidores de la UIS:

```
[root@ACER8448 root]# nmap -o 192.168.1.133
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
WARNING: No targets were specified, so 0 hosts scanned.
Nmap run completed -- 0 IP addresses (0 hosts up) scanned in 0 seconds
[root@ACER8448 root]# nmap -sF 192.168.1.133 0/24
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
All 1601 scanned ports on (192.168.1.133) are: closed
Host (0.0.0.0) seems to be a subnet broadcast address (returned 1 extra pings). Skipping host.
sendto in send_ip_raw: sendto(4, packet, 28, 0, 0.0.0.1, 16) => Invalid argumentSleeping 15 seconds then retrying
sendto in send_ip_raw: sendto(4, packet, 28, 0, 0.0.0.1, 16) => Invalid argumentSleeping 60 seconds then retrying
sendto in send_ip_raw: sendto(4, packet, 28, 0, 0.0.0.1, 16) => Invalid argumentSleeping 240 seconds then retrying
[4]+ Stopped nmap -sF 192.168.1.133 0/24
[root@ACER8448 root]# nmap -sF 192.168.19.6/24
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
All 1601 scanned ports on p880.uis.edu.co (192.168.19.1) are: closed
Interesting ports on condor.uis.edu.co (192.168.19.2):
(The 1583 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
79/tcp open finger
80/tcp open http
109/tcp open pop-2
110/tcp open pop-3
111/tcp open sunrpc
143/tcp open imap2
443/tcp open https
875/tcp open unknown
993/tcp open imaps
995/tcp open pop3s
6000/tcp open X11
10000/tcp open snet-sensor-mgmt
32770/tcp open sometimes-rpc3
All 1601 scanned ports on pelicano.uis.edu.co (192.168.19.6) are: closed
Interesting ports on tucan.uis.edu.co (192.168.19.7):
(The 1593 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
25/tcp open smtp
80/tcp open http
110/tcp open pop-3
111/tcp open sunrpc
143/tcp open imap2
993/tcp open imaps
995/tcp open pop3s
Interesting ports on copeton.uis.edu.co (192.168.19.8):
(The 1582 ports scanned but not shown below are in state: closed)
Port State Service
11/tcp open systat
15/tcp open netstat
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
79/tcp open finger
80/tcp open http
110/tcp open pop-3
111/tcp open sunrpc
113/tcp open auth
143/tcp open imap2
513/tcp open login
514/tcp open shell
697/tcp open unknown
698/tcp open unknown
3306/tcp open mysql
8080/tcp open http-proxy
```

All 1601 scanned ports on faisan.uis.edu.co (192.168.19.9) are: closed
Interesting ports on cormoran.uis.edu.co (192.168.19.12):
(The 1585 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
80/tcp open http
110/tcp open pop-3
111/tcp open sunrpc
443/tcp open https
742/tcp open netrcs
761/tcp open kpasswd
993/tcp open imaps
995/tcp open pop3s
2049/tcp open nfs
3306/tcp open mysql
6000/tcp open X11
8009/tcp open ajp13
8080/tcp open http-proxy
Interesting ports on dodo.uis.edu.co (192.168.19.15):
(The 1588 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
79/tcp open finger
80/tcp open http
111/tcp open sunrpc
139/tcp open netbios-ssn
443/tcp open https
901/tcp open samba-swat
5432/tcp open postgres
6000/tcp open X11
8009/tcp open ajp13
8080/tcp open http-proxy
10000/tcp open snet-sensor-mgmt
All 1601 scanned ports on dsi01.uis.edu.co (192.168.19.17) are: closed
Interesting ports on quetzal.uis.edu.co (192.168.19.18):
(The 1589 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
23/tcp open telnet
79/tcp open finger
80/tcp open http
110/tcp open pop-3
443/tcp open https
513/tcp open login
514/tcp open shell
1024/tcp open kdm
1025/tcp open NFS-or-IIS
5432/tcp open postgres
6000/tcp open X11
Interesting ports on albatros.uis.edu.co (192.168.19.32):
(The 1584 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
109/tcp open pop-2
110/tcp open pop-3
111/tcp open sunrpc
139/tcp open netbios-ssn
143/tcp open imap2
443/tcp open https
901/tcp open samba-swat
3306/tcp open mysql

5432/tcp open postgres
6000/tcp open X11
8080/tcp open http-proxy
10000/tcp open snet-sensor-mgmt
Interesting ports on garza.uis.edu.co (192.168.19.33):
(The 1585 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
80/tcp open http
106/tcp open pop3pw
110/tcp open pop-3
139/tcp open netbios-ssn
143/tcp open imap2
311/tcp open asip-webadmin
389/tcp open ldap
427/tcp open svrloc
445/tcp open microsoft-ds
625/tcp open unknown
687/tcp open unknown
3306/tcp open mysql
5900/tcp open vnc
All 1601 scanned ports on carpintero.uis.edu.co (192.168.19.51) are: closed
Interesting ports on tux.uis.edu.co (192.168.19.52):
(The 1559 ports scanned but not shown below are in state: closed)
Port State Service
1/tcp open tcpmux
7/tcp open echo
9/tcp open discard
11/tcp open systat
15/tcp open netstat
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
70/tcp open gopher
79/tcp open finger
80/tcp open http
109/tcp open pop-2
110/tcp open pop-3
111/tcp open sunrpc
119/tcp open nntp
138/tcp open netbios-dgm
139/tcp open netbios-ssn
143/tcp open imap2
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
540/tcp open uucp
587/tcp open submission
635/tcp open unknown
1080/tcp open socks
1524/tcp open ingreslock
2000/tcp open callbook
2001/tcp open dc
4000/tcp open remoteanything
6001/tcp open X11:1
6667/tcp open irc
12345/tcp open NetBus
12346/tcp open NetBus
27665/tcp open Trinoo_Master
31337/tcp open Elite
32771/tcp open sometimes-rpc5
32772/tcp open sometimes-rpc7
32773/tcp open sometimes-rpc9
32774/tcp open sometimes-rpc11

```
54320/tcp open bo2k
Interesting ports on pinguino.uis.edu.co (192.168.19.54):
(The 1589 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop-3
111/tcp open sunrpc
143/tcp open imap2
443/tcp open https
993/tcp open imaps
995/tcp open pop3s
6000/tcp open X11
Interesting ports on garceta.uis.edu.co (192.168.19.56):
(The 1592 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
80/tcp open http
111/tcp open sunrpc
443/tcp open https
993/tcp open imaps
995/tcp open pop3s
3306/tcp open mysql
6000/tcp open X11
Interesting ports on condorito.uis.edu.co (192.168.19.57):
(The 1585 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
79/tcp open finger
80/tcp open http
98/tcp open linuxconf
99/tcp open metagram
110/tcp open pop-3
113/tcp open auth
139/tcp open netbios-ssn
143/tcp open imap2
515/tcp open printer
2003/tcp open cfingerd
3306/tcp open mysql
5432/tcp open postgres
All 1601 scanned ports on kiwi.uis.edu.co (192.168.19.63) are: closed
All 1601 scanned ports on tyrano.uis.edu.co (192.168.19.70) are: closed
All 1601 scanned ports on o200.uis.edu.co (192.168.19.80) are: closed
Nmap run completed -- 256 IP addresses (20 hosts up) scanned in 339 seconds
```

Nivel de riesgo: Medio.

Costo asociado: Un atacante merodea en busca de información, actúa como un ladrón que palpa las paredes a la búsqueda de puertas o ventanas que pueda violar para cometer el ilícito. La exploración de puertos le permite a un atacante obtener listas de direcciones IP, que lo llevan a conocer información importante como nombres de servidores DNS y de correo, de empleados, números telefónicos entre otros, luego mediante diferentes maniobras determinan cuales sistemas se encuentran abiertos, para planear el ataque o estrategia que le permita acceder al sistema objetivo.

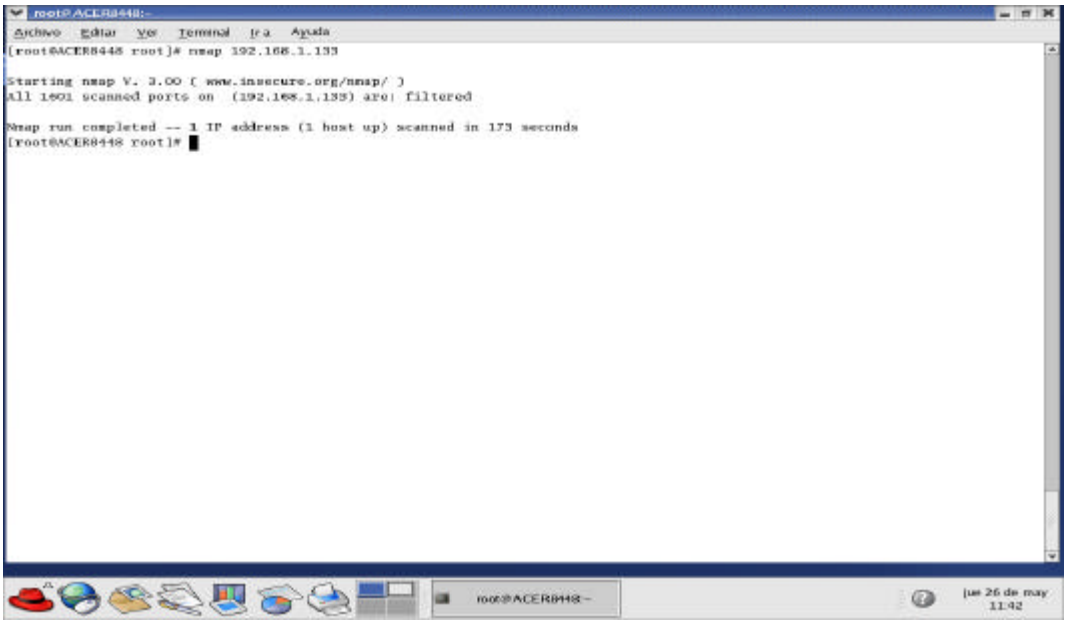
Debilidades encontradas en el Firewall de la UIS (amenazas provenientes externamente):

Amenaza 22. Exploración de puertos al Firewall de la UIS y routers CISCO ETB y TELECOM.

Nivel de riesgo: Medio.

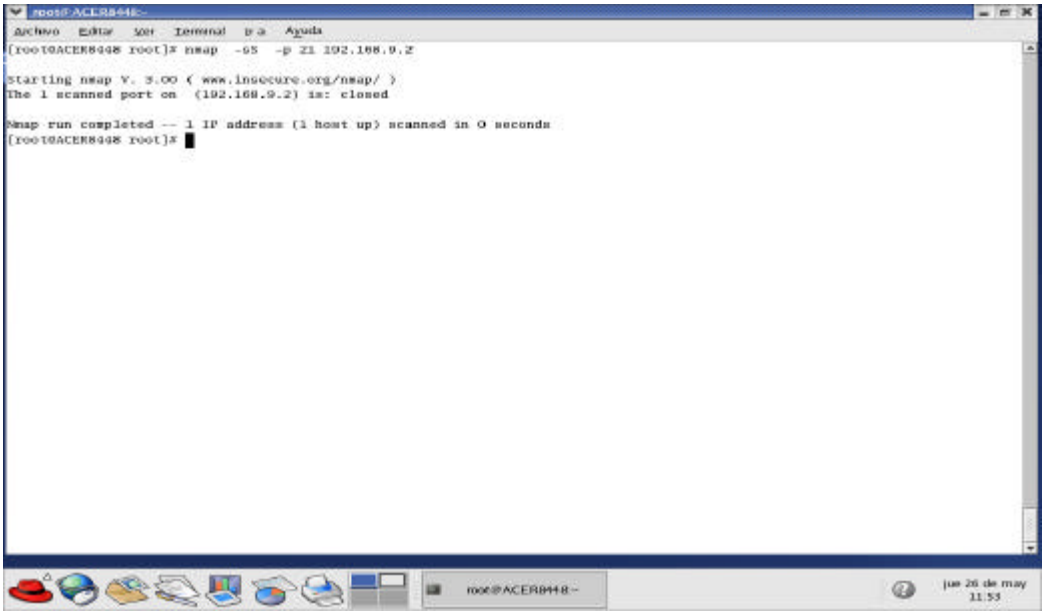
Costo Asociado: La conexión externa actualmente de la UIS se puede observar en la Figura 11. Está conformada por los proveedores de servicio de Internet de la Universidad; dentro de esta infraestructura se observa el dispositivo de protección exterrna firewall CISCO PIX 515, propiedad de la universidad, además de dispositivos Cisco 3360 propiedad de ETB, Cisco 3320 propiedad de la UIS, Cisco 7600 propiedad de Telecom, para lo cual se efectuaron pruebas de exploración a sus puertos dando como resultado los siguientes:

Figura 30. Exploración de Puertos E0 Firewall Cisco Pix-515



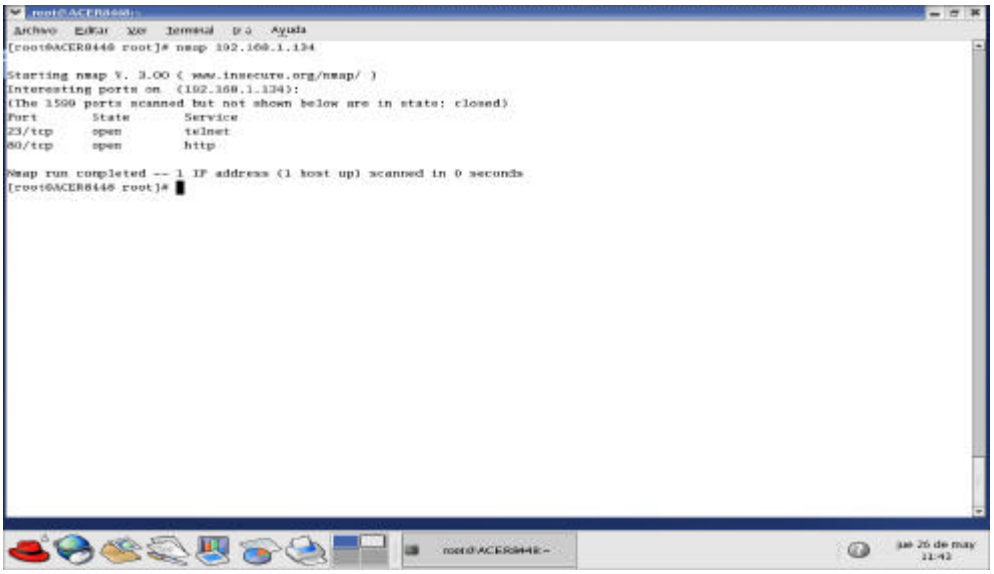
Fuente: Autor del proyecto.

Figura 31. Exploración de Puertos (21 FTP del Firewall)



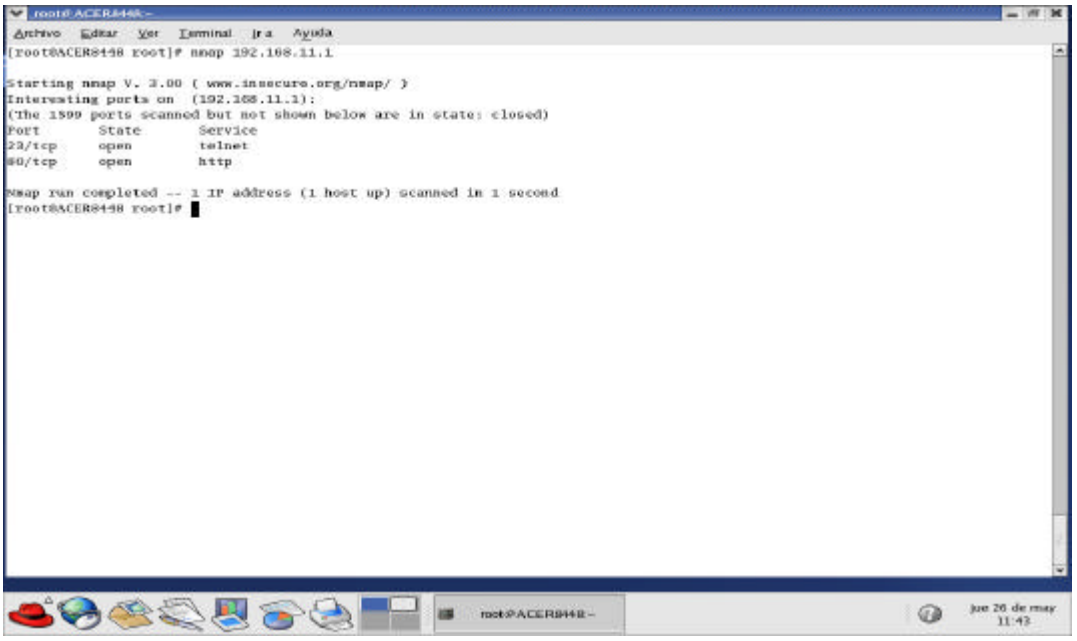
Fuente: Autor del proyecto.

Figura 32. Exploración de Puertos Cisco 3360 de ETB



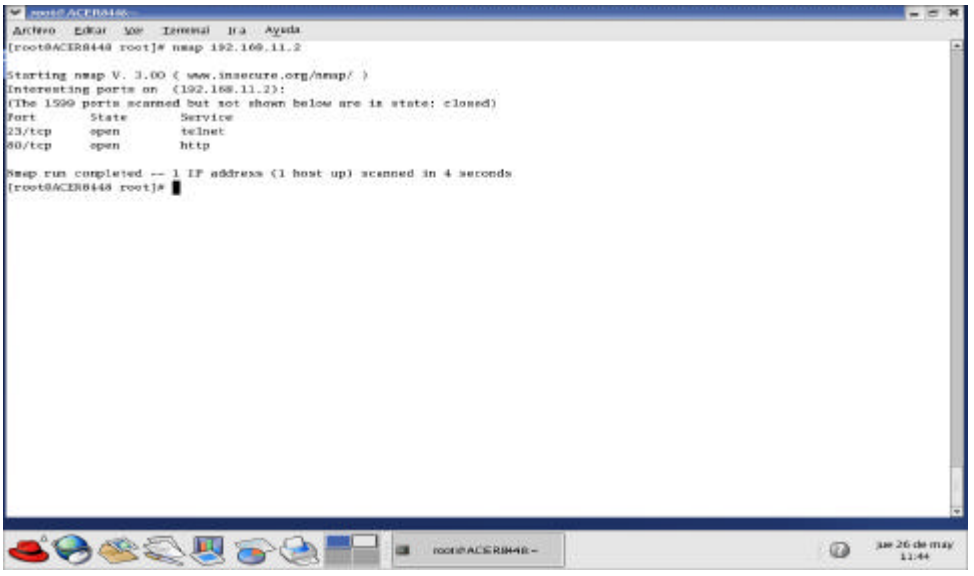
Fuente: Autor del proyecto.

Figura 33. Exploración de Puertos Ethernet 0 del Cisco 3360 de ETB



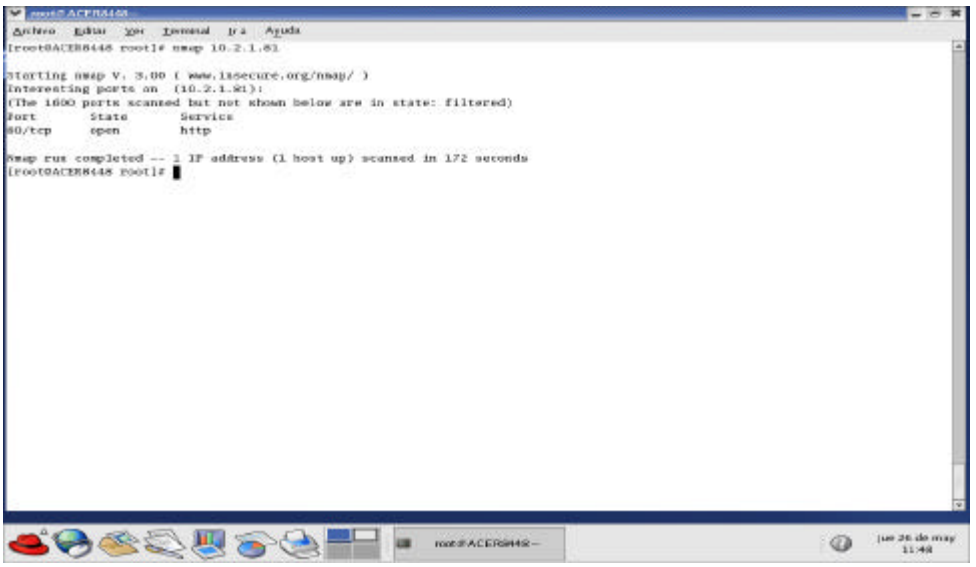
Fuente: Autor del proyecto.

Figura 34. Exploración de Puertos Cisco 3320 FE0/1 UIS



Fuente: Autor del proyecto.

Figura 35. Exploración de Puertos Cisco 7600 de Telecom



Fuente: Autor del proyecto.

- VULNERABILIDADES DE LOS SERVIDORES DE CORREO DE LA UIS.

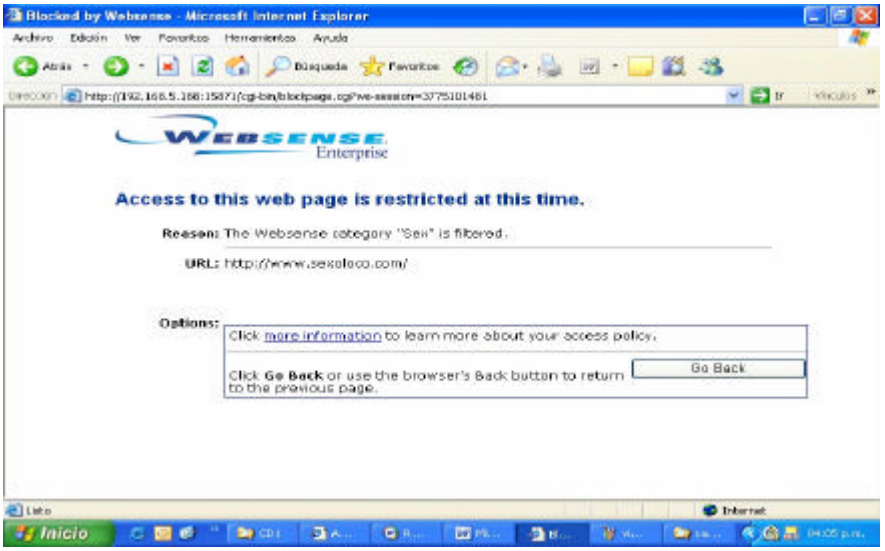
Amenaza 23. Violación al WEBSENSE (mecanismo que administra, controla y optimiza el uso de ancho de banda de acceso a Internet.
Nivel de riesgo: Medio

Costo Asociado: La UIS posee y paga derechos para usar un software para el control de contenidos de la web denominado WEBSENSE, con el objetivo de evitar que tanto sus empleados como los estudiantes puedan acceder a páginas de ocio y entretenimiento en tiempos laborales y de estudio, además *"el hecho de que la universidad sea pública, significa que se debe a la sociedad, por lo que no se debe permitir ningún tipo de usos indebidos"*[23]. Desafortunadamente en este trabajo de investigación se detectó la violación del filtro por algunos estudiantes de la institución en la siguiente forma:

1. Las páginas en las que frecuentemente los estudiantes intentan acceder son las de ocio y en especial páginas pornográficas. Si el estudiante intenta acceder normalmente el filtro WEBSENSE les impide el acceso respondiendo con el siguiente mensaje:

[23] Palabras textuales dadas a CONEXXION- EISI por el Ing MsC Benjamín Pico Merchan, actualmente administrador de la red de datos institucional de la Universidad en respuesta a una entrevista concedida a Diana Valbuena y Sebas Knight : Redes UIS al desnudo, Acerca de la infraestructura de red de la Universidad y del popular Websense.

Figura 36. Paso 1 – Violación del WEBSENSE



Fuente: Autor del proyecto.

2. Por lo tanto algunos se las ingenian para violar estos filtros accediendo primero a páginas de proxies libres como por ejemplo http://anonymouse.ws/. Posteriormente escogen el idioma inglés.

Figura 37. Paso 2 – Violación del WEBSENSE

Fuente: Autor del proyecto.

3. Luego se presentan tres opciones la primera AnonEmail para envío de correos, la segunda AnonWWW para acceder a páginas y la tercera AnonNews para noticias de proxies. Escogen AnonWWW.

Figura 38. Paso 3 – Violación del WEBSENSE

Fuente: Autor del proyecto.

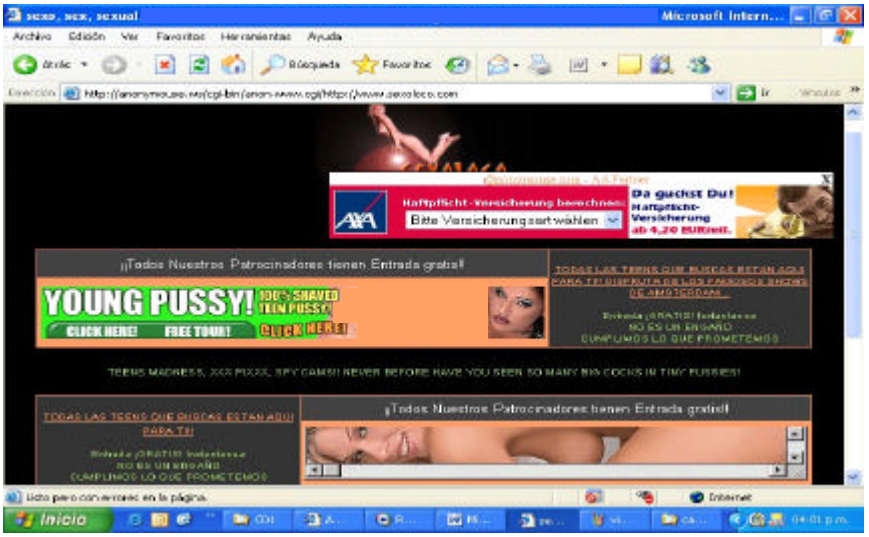
4. Introducen la dirección de la página que quieren acceder en este caso URL: http://www.sexoloco.com.

Figura 39. Paso 4 – Violación del WEBSENSE

Fuente: Autor del proyecto.

5. Dan click en surf anonymously para acceder a la página prohibida y efectivamente logran acceder la página y violar el filtro de la universidad.

Figura 40. Paso 5 – Violación del WEBSENSE



Fuente: Autor del proyecto.

Amenaza 24. Violación de los servidores de correo de la UIS (cóndor y albatros).

Nivel de Riesgo: Medio.

Costo Asociado: En la UIS como en cualquier organización o persona tiene derecho a su privacidad, pero se encontró lo siguiente:

Para demostrar la vulnerabilidad del servidor de correo de la universidad se intentó acceder a albatros y a cóndor obteniendo los siguientes resultados:

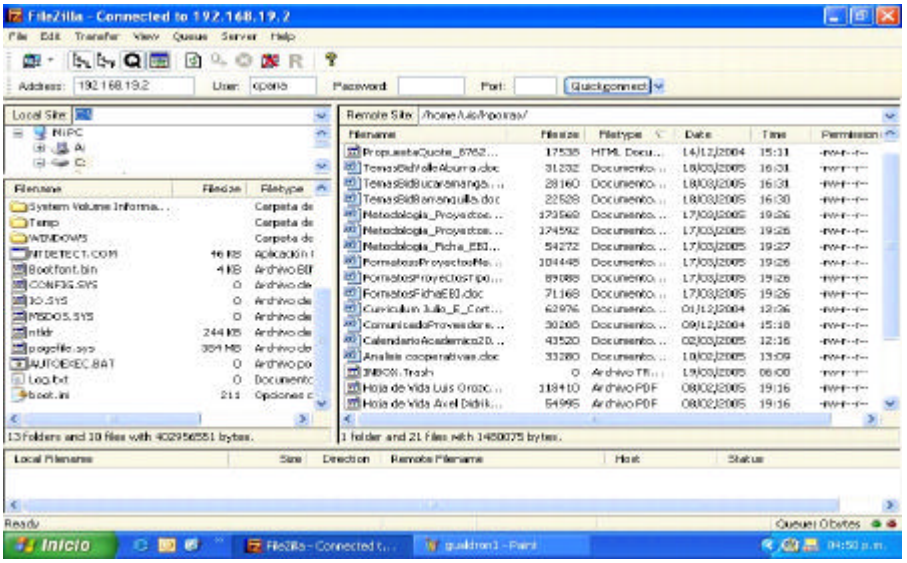
Utilizando una cuenta de la Universidad se efectuó la siguiente maniobra:

1. Se instaló desde un equipo de la universidad el software FileZilla_2_2_7a_setup que es un programa para manejar archivos mediante ftp.

2. Empleando el anterior software nos conectamos al servidor de correo Cóndor que tiene la IP 192.168.19.2 como un usuario válido.

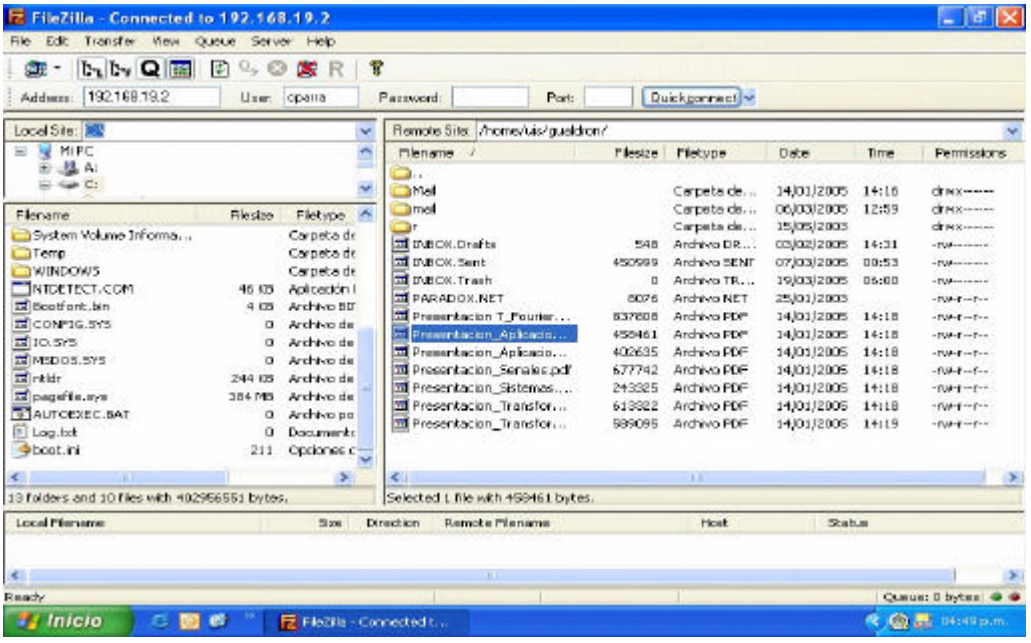
3. Se observa que podemos desplazarnos a carpetas privadas de profesores ubicadas en la dirección /home/uis/. En este caso accedimos a archivos de correo del docente Hernán Porras ubicado en /home/uis/hporras/ y también al del docente Oscar Gualdrón ubicado en /home/uis/gualdron/.

Figura 41. Paso 1 – Violación servidor de correo - Cóndor



Fuente: Autor del proyecto

Figura 42. Paso 2 – Violación servidor de correo Cóndor

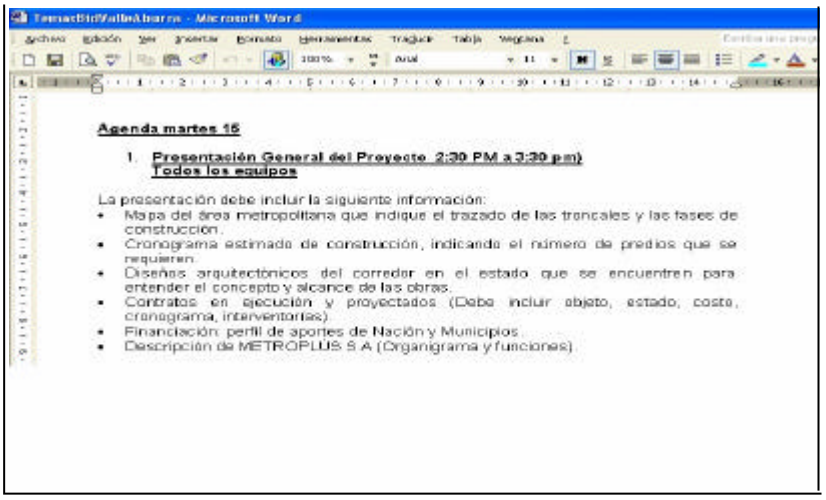


Fuente: Autor del proyecto

Por lo tanto al observar los archivos en los respectivos directorios de los docentes, fácilmente con el software FileZilla podemos copiarlos, bajarlos al

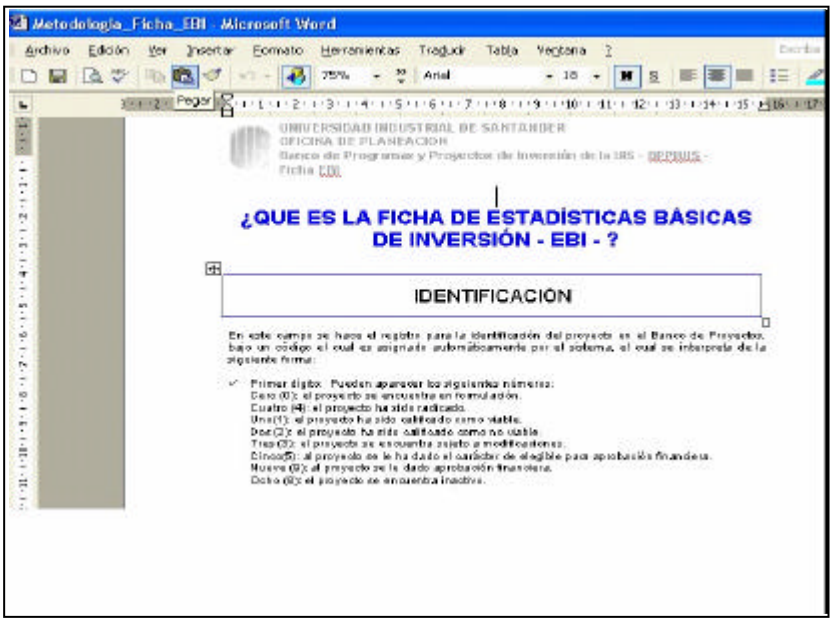
disco duro y observar posteriormente el contenido, como se puede observar con los del directorio del docente Hernán Porras:

Figura 43. Paso 3 – Violación servidor de correo Cóndor- Archivos Docente Hernán Porras



Fuente: Autor del proyecto

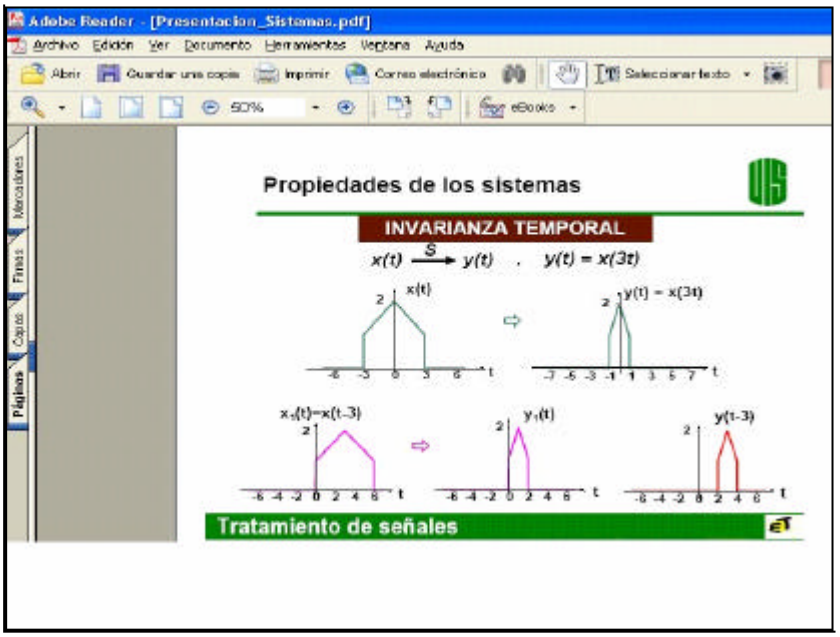
Figura 44. Violación servidor de correo Cóndor- Archivos Docente Hernán Porras



Fuente: Autor del proyecto

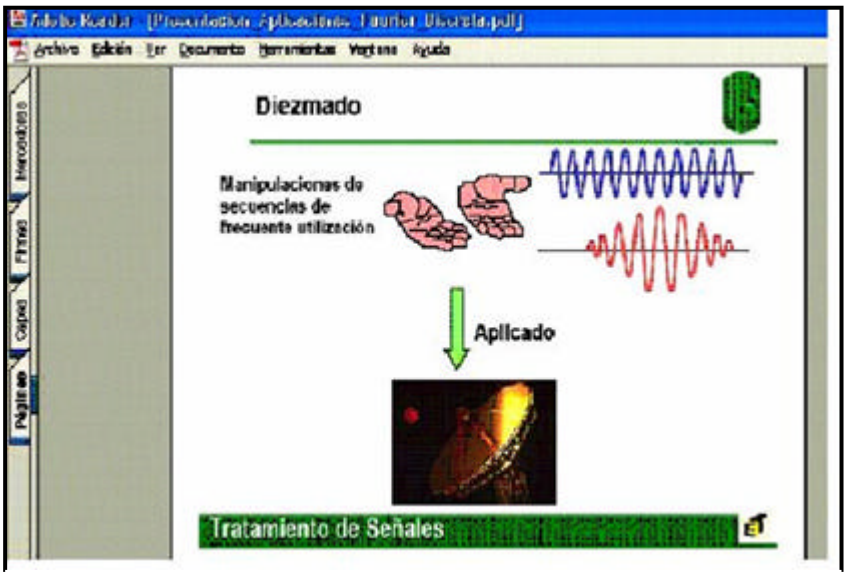
El mismo proceso se efectuó con los archivos Docente Oscar Gualdrón y se obtuvieron los siguientes archivos:

Figura 45. Violación servidor de correo Cóndor- Archivos Docente Oscar Gualdrón



Fuente: Autor del proyecto

Figura 46. Violación servidor de correo Cóndor- Archivos Docente Oscar Gualdrón



Fuente: Autor del proyecto

Debilidades encontradas en el software de Aplicación, programas fuente y objeto.

Amenazas generales encontradas sobre el software de aplicación y los programas:

Amenaza 25. Alteración malintencionada del software de aplicación, mediante la inclusión dentro del código de programas que se instalan como: virus, caballos de troya u otras amenazas.

Exploits de vulnerabilidades conocidas en programas y servicios

Nivel de Riesgo: Alto

Costo Asociado: Los fallos y errores de diseño no sólo en las aplicaciones sino también en los núcleos de los sistemas operativos son fuentes de amenazas a la seguridad de todo sistema informático, por tanto los errores o bugs en el código fuente de las aplicaciones constituyen una de las amenazas a la seguridad que más problemas han causado a la comunidad de la seguridad informática. Generalmente estas complicaciones no se originan por falta de conocimiento en la realización de programas seguros, sino más bien en que resulta casi imposible no cometer alguna equivocación en miles de líneas de código.

Con frecuencia muchos programas son afectados por uno de los errores más comunes y utilizados por atacantes como es el desbordamiento de pila (snack smashing), también conocido como buffer overflow). A pesar de que los programas en especial los setuidados, son en la actualidad más seguros; es muy frecuente que un atacante intente acceder a un sistema consiguiendo privilegios de administrador a través de un buffer overflow.

Otra amenaza a la seguridad son los exploits, disponibles en Internet (programas que aprovechan un error en otro programa o servicio para violar la política de seguridad del sistema y ganar privilegios sobre éste), existen para casi todas las versiones de Unix e incluyen el código necesario para ejecutar shells sobre cualquier sistema operativo y arquitectura.

Debilidades encontradas en los Datos.

Amenazas generales encontradas en los datos:

Amenaza 26. Divulgación, modificación, interceptación, pérdida total o parcial de los datos.

Nivel de Riesgo: Alto

Costo Asociado: La interceptación o eavesdropping, (conocida también como passive wiretapping) se puede definir como el proceso mediante el cual un agente obtiene o captura información (en claro o cifrada) que no le iba dirigida. Lo más peligroso del eavesdropping es que es muy difícil de detectar mientras que se produce, ya que este tipo de ataque se comporta en un comienzo como un ataque pasivo, es decir que el atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta, luego el mismo atacante emplea la información capturada, convirtiendo el ataque en activo. Un mecanismo de interceptación comúnmente utilizado es el sniffing.

La información almacenada en el sistema puede perderse o modificarse debido a varias causas como:

- Daños en los componentes hardware de la máquina.

- Borrado o modificación, accidental o intencional, de los datos almacenados en la base de datos.

- Pérdida o modificación de los programas de aplicación almacenados en los discos duros de la máquina.

Ante estas problemáticas las copias de seguridad (backups) son frecuentemente el único mecanismo de recuperación que poseen los administradores para restaurar una máquina a su estado de normal funcionamiento. Por tanto, es de suma importancia una correcta política para realizar, almacenar y restaurar los backups, resultando vital en la planificación de la seguridad de todo sistema.

Debilidades encontradas en los Usuarios.

Amenazas generales encontradas en los Usuarios:

Amenaza 27. Atacante interno, sistema de autenticación de unix, revelado de contraseñas.

Nivel de Riesgo: Alto

Costo Asociado: Los fraudes, robos sabotajes o accidentes relacionados con los sistemas informáticos son provocados por el propio personal de la organización dueña de dichos sistemas. Por lo tanto la mayor amenaza a los equipos de la organización surge principalmente por parte personas que trabajan o han trabajado para la misma. Es así como las personas que han trabajado con los administradores o programadores de una organización pueden llegar a conocer el sistema perfectamente, sus fortalezas y debilidades; por lo tanto un ataque realizado por esa persona va a ser probablemente un ataque mucho más

peligroso porque puede ser más directo, difícil de detectar, y efectivo, que el que pueda propiciar un atacante externo que necesita recopilar información, intentar probar fallos de seguridad o conseguir privilegios para poder ejecutarlo. Si analizamos la motivación que pueda tener una persona para atacar su propia organización son diversos, ya que pueden ser económicos, inconformidad con el cargo, desafío personal, etc, la realidad es que este tipo de ataques ocurren y son muy frecuentes.

En los sistemas Unix cada usuario para acceder al sistema posee un nombre de entrada o login y una clave o password; los cuales se almacenan por lo general en el fichero /etc/passwd. Dicho archivo contiene una línea por usuario que contiene la información necesaria para que los usuarios puedan conectar al sistema y trabajar en él. Los campos son separados mediante el carácter ":". En el fichero /etc/passwd se encuentran entradas como las siguientes:

publico:x:1500:100:PUBLICO:/disco2/biblio:/bin/sh

En la que el primer campo aparece el login del usuario y su clave cifrada; luego el tercer campo el identificador de usuario, el cuarto campo el identificador del grupo respectivamente, el quinto campo es conocido como GECOS contiene información administrativa sobre la identidad real del usuario como su nombre o teléfono. Finalmente los dos últimos campos corresponden al directorio del usuario ($HOME) y al shell que le ha sido asignado.

El sistema operativo Unix no diferencia a sus usuarios por su nombre de entrada al sistema, sino por medio del UID del usuario; el login es empleado más bien por comodidad de los usuarios ya que es más fácil de recordar que un UID, principalmente si se tienen cuentas en muchas máquinas, cada una con un UID diferente, pero si en /etc/passwd llegan a existir dos entradas con el mismo UID, Unix los tomaría como el mismo usuario, aunque tengan un login y password diferente: por lo tanto si dos usuarios tienen asignado el UID 0, ambos tendrán privilegios de superusuario, sin importar el login que utilicen. Esta situación es aprovechada por atacantes que logran conseguir privilegios de administrador en una máquina, logrando añadir una línea a /etc/passwd con un nombre de usuario normal pero con el UID 0; garantizando con esta maniobra la entrada al sistema como administradores, en caso de ser descubiertos, para borrar los rastros o huellas. La detección de esta línea es difícil especialmente en sistemas con gran números de usuarios, pero para detectar las cuentas con privilegios en la máquina se puede utilizar el comando: awk –F:'$3==0 {print $1}' /etc/passwd.

Respecto a los ataques de texto cifrado escogido estos conforman la principal amenaza al sistema de autenticación de Unix; aunque no es posible descifrar una

contraseña, si es fácil cifrar una palabra junto a un determinado salt[24], y comparar el resultado con la cadena almacenada en el fichero de claves, generalmente ubicado en /etc/passwd. De esta manera, el atacante leerá el fichero de claves y luego empleará un programa adivinador de contraseñas conocido también como crackeador, el cual cifrará todas las palabras de un fichero denominado diccionario, comparando los resultados obtenidos en este proceso con la clave cifrada del fichero de contraseñas, si los resultados coinciden el atacante ha obtenido una clave para acceder al sistema.

[24] Para el cifrado de las claves de acceso de los usuarios, Unix emplea un criptosistema irreversible que emplea la función estándar de C crypt(3), basada en el algoritmo DES. Esta función toma como clave los primeros ocho caracteres de la contraseña elegida por el usuario (si la longitud es menor se completa con ceros) para cifrar un bloque de texto en claro de 64 bits puestos a cero; para evitar que dos passwords iguales resulten iguales en un mismo texto cifrado, se realiza una permutación durante el proceso de cifrado elegida de forma automática y aleatoria para cada usuario, basada en un campo formado por un número de 12 bits (con lo que conseguimos 4096 permutaciones diferentes) llamado **salt**.

3. PROPUESTA DE DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

Luego de conocer la infraestructura computacional y de efectuar el estudio y análisis de vulnerabilidades encontradas en la UIS, se procede con este capítulo a proponer el modelo de seguridad informático.
Este capítulo tiene como objetivos:

- Diseñar un modelo de seguridad para la mitigación de la vulnerabilidad de la Red de Datos Institucional de la Universidad Industrial de Santander.

- Estimar el presupuesto de la implantación del Modelo para la Universidad Industrial de Santander.

3.1 AUDITORIA

Auditoría Informática. La Auditoría Informática es el proceso de recolección y evaluación de evidencia para determinar sí un sistema automatizado: salvaguarda activos (daños, destrucción, uso no autorizado, robo), mantiene la integridad de los datos (oportuna, precisa, confiable, completa), alcanza metas organizacionales (contribución de la función Informática), consume recursos eficientemente (utiliza los recursos adecuadamente en el procesamiento de la información).

Es también conocida en nuestro medio con el nombre de Auditoría de Sistemas, debido a que la información se convirtió en uno de los activos más importantes de las empresas, lo cual se puede confirmar al considerar el hecho de que si se queman las instalaciones físicas de cualquier organización, sin que sufran daños los ordenadores, servidores o equipo de cómputo, la entidad podría retomar su operación normal en un menor tiempo, que si ocurre lo contrario. A raíz de esto, la información adquiere gran importancia en la empresa moderna debido a su poder estratégico y a que se invierten grandes sumas de dinero y tiempo en la creación de sistemas de información con el fin de obtener una mayor productividad.

Otro factor que influyó grandemente en el nacimiento de la Auditoría Informática fue el uso de la tecnología y sistemas computarizados para el procesamiento de la información, lo cual ha tenido una importante repercusión sobre la disciplina contable, pues la mayoría de las operaciones financieras han recibido la influencia de la informática.

Alcance de la Auditoría Informática. El alcance de la Auditoría Informática no es nada más que la precisión con que se define el entorno y los límites en que va a desarrollarse la misma y se complementa con los objetivos establecidos para la revisión. El alcance de la Auditoría Informática deberá definirse de forma clara en el Informe final, detallando no solamente los temas que fueron examinados, sino también indicando cuales se omitieron.

Tipos de Auditoría Informática. El Departamento de Informática o Sistemas desarrolla diversas actividades y sobre la base de estas se han establecido las principales divisiones de la Auditoría Informática, las cuales son: de Producción u Explotación, Desarrollo de Proyectos, de Sistemas, de Comunicaciones y Redes y de Seguridad. A continuación repasaremos brevemente cada una.

Auditoría Informática de Producción o Explotación. En algunos casos también conocida como de Explotación u Operación, se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc.

La producción, operación o explotación informática dispone de una materia prima, los datos, que son necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas y obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar la producción, operación o explotación consiste en revisar las secciones que la componen y sus interrelaciones, las cuales generalmente son: planificación, producción y soporte técnico.

Auditoría Informática de Desarrollo de Proyectos. La función de desarrollo es una evolución del llamado análisis y programación de sistemas, y abarca áreas, como son: requerimientos del usuario y del entorno, análisis funcional, diseño, análisis orgánico (preprogramación y programación), pruebas entrega a explotación o producción y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, ya que en caso contrario, los costos pueden excederse, puede producirse la insatisfacción del usuario.

La auditoría en este caso deberá principalmente comprobar la seguridad de los programas en el sentido de garantizar que lo ejecutado por la máquina sea exactamente lo previsto o lo solicitado inicialmente.

Auditoría Informática de Sistemas. Se ocupa de analizar y revisar los controles y efectividad de la actividad que se conoce como técnicas de sistemas en todas

sus facetas y se enfoca principalmente en el entorno general de sistemas, el cual incluye sistemas operativos, software básicos, aplicaciones, administración de base de datos, etc.

Auditoría Informática de Comunicaciones y Redes. Este tipo de revisión se enfoca en las redes, líneas, concentradores, multiplexores, etc. Así pues, la Auditoría Informática ha de analizar situaciones y hechos algunas veces alejados entre sí, y está condicionada a la participación de la empresa telefónica que presta el soporte. Para este tipo de auditoría se requiere un equipo de especialistas y expertos en comunicaciones y redes.

El auditor informático deberá indagar sobre los índices de utilización de las líneas contratadas, solicitar información sobre tiempos de desuso; deberá proveerse de la topología de la red de comunicaciones actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. Por otro lado, será necesario que obtenga información sobre la cantidad de líneas existentes, cómo son y donde están instaladas, sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas, pues la contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (pantallas, servidores de redes locales, computadoras, impresoras, etc.).

Auditoría de la Seguridad Informática. La Auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

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

El auditar la seguridad de los sistemas, también implica que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.

Auditoría Informática para Aplicaciones en Internet. En este tipo de revisiones, se enfoca principalmente en verificar los siguientes aspectos, los cuales no puede pasar por alto el auditor informático:

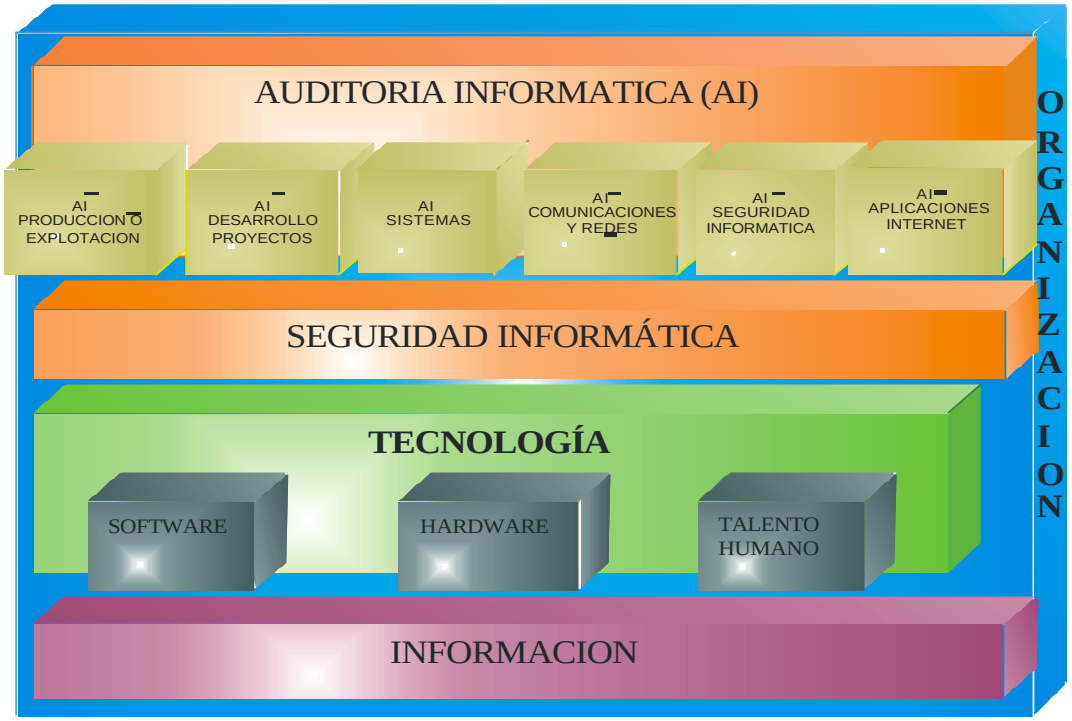
- Evaluación de los riesgos de internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.

- Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.

- Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

El siguiente esquema pretende ubicar e ilustrar los alcances tanto de la auditoría informática como de la seguridad informática:

Figura 47. La Auditoría Informática y la Seguridad Informática en la Organización



Fuente: Autor del Proyecto

3.2 CONCEPTO DE MODELO

El nacimiento de un modelo de una cosa o hecho, se da en el intento de la conquista conceptual de la realidad. La formación de cada modelo comienza por simplificaciones, pero la sucesión histórica de los mismos es un proceso de complejidad. Se construyen modelos conceptuales y se sabe que ellos sólo dan una imagen simbólica de la realidad, aún cuando se intente por medio de complicaciones acercarlos a ella; entonces para qué construirlos y desgastarse en

algo que de antemano se sabe no es real?, o qué hacer para que alguno tenga sentido, entendiendo por esto: aproximación o validación en algunos casos reales?. La primera pregunta se puede sólo satisfacer en parte con la certeza de que es preciso iniciar el proceso de conceptualizar por alguna parte, y que mejor que la creación de esquemas sencillos de interpretar que puedan conducirnos a deducciones de carácter más real, que abran camino para abordar esquemas más completos; la segunda puede verse como una invitación a involucrar la razón pura, la intuición, la contrastación empírica y la observación, al desarrollo de tales modelos.

El proceso de generación de modelos se puede visualizar como un apresar la realidad, que empieza por apartar información, a la cual se agregan elementos hipotéticos con una intención realista, con ellos se construye un objeto modelo esquemático y éste se lleva a una teoría susceptible de ser confrontada con hechos.

Modelos de Seguridad Informática. Para poder proponer el modelo de seguridad para la Universidad Industrial de Santander se hizo necesario indagar acerca de las bases conceptuales que permitieran soportarlo, para esto se encontró que las organizaciones necesitan estándares de seguridad de la información, debido a que, las solas políticas de seguridad no son suficientes, ya que estas establecen la necesidad de seguridad de la información, pero no especifican lo que debe hacerse para implementarlas. Ésta es la función de los Estándares de Seguridad de la Información, que establecen lo siguiente:

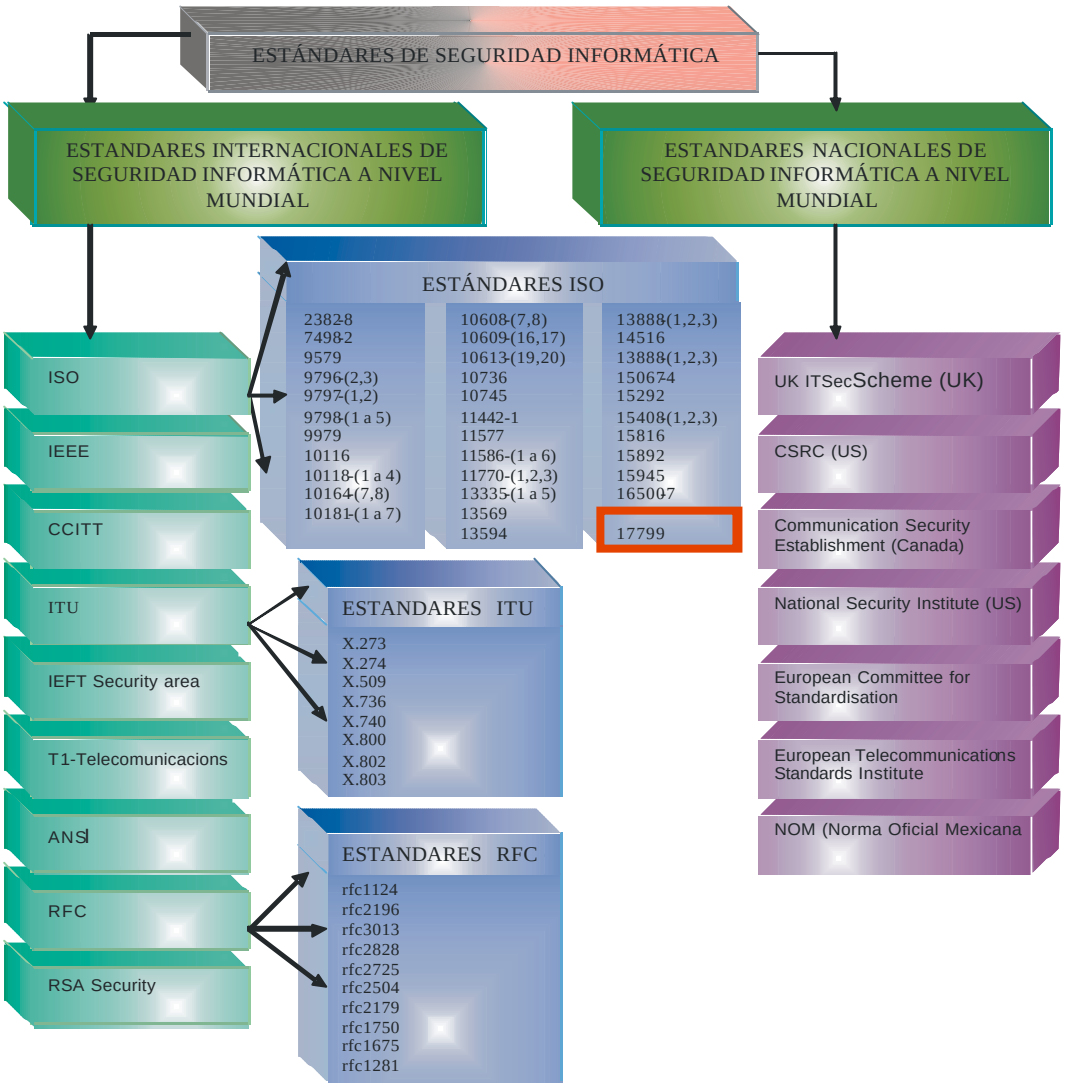
- Lo que se debe hacer

- Los controles de seguridad que se requieren

- Controles de seguridad adecuados que se apliquen a cada elemento del entorno de protección de la información

Al tener claridad acerca del propósito de los estándares, surge el dilema de la escogencia del estándar más adecuado y más reconocido por las organizaciones a nivel mundial, para lo cual se indagó y obtuvo el panorama de estándares a nivel mundial (ver figura 45).

Figura 48. Estándares de Seguridad Informática



Fuente: FARIAS, M. *La Importancia de los Estándares en Seguridad Informática.* Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA), Universidad La Salle, email: **elinos@ci.ulsa.mx**, Grupo de Seguridad de Internet-2 México, **http://seguridad.internet2.ulsa.mx/**

Cuadro 16. Estándares de seguridad informática a nivel mundial

ESTANDARES DE SEGURIDAD INFORMÁTICA A NIVEL MUNDIAL:	
ISO	Internacional Organization for Standardization
IEEE	Consultative Committee on International Telegraphy and Telephony
CCITT	Consultative Committee on International Telegraphy and Telephony
ITU	International Telecommunication Union
IETF	The Internet Engineering Task Force
T1-Telecomunicacions	Standards Committee T1 Telecomunicacions (USA)
ANSI	American National Standards Institute (USA).
RFC	Internet Requests for Comments
RSA Security	Creada desde el año 1982 y con la implementación del algoritmo para encriptamiento de datos, desarrollado por Ron Rivest, Adi Shamir, Leonard Adleman. Su estándar es utilizado por numerosos sectores económicos, para custodiar su información e incluso, el Gobierno Francés lo emplea como estándar, para proteger sus comunicaciones (USA).
ESTANDARES DE SEGURIDAD INFORMATICA NACIONAL A NIVEL MUNDIAL	
UK ITSec Scheme (UK)	Information Technology Security Evaluation and Certification Scheme (Reino Unido).
CSRC	China Securities Regulatory Commission (China)
Communication Security Establishment (Canada)	Estándar canadiense
National Security Institute	Estándar Norteamericano (USA).
European Committee for Standardisation	Estándar europeo
European Telecommunications Standards Institute	Estándar europeo
NOM	Norma Oficial Mexicana : Estándar mexicano.

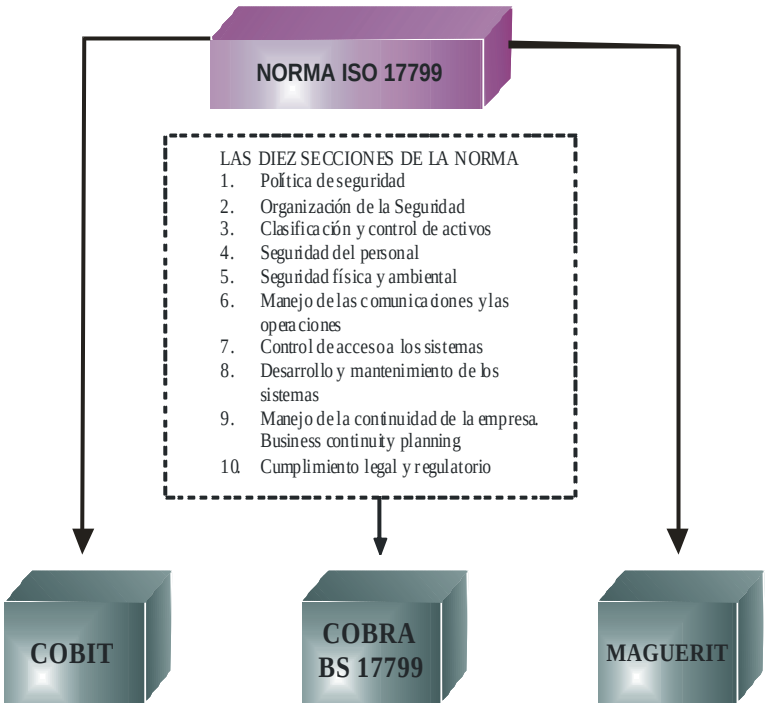
Fuente: Autor del proyecto.

Generalmente son validados por CISA- Certified Information System Auditor, que tienen como función validar el estado de la seguridad informática frente a estándares y mejores prácticas internacionales. Dentro de estos modelos tenemos los más sobresalientes los siguientes:

- COBIT
- ISO 17779
- MAGUERIT
- Common Criteria Model
- Information Security Governance
- Federal Information System Control audit. Manual

Estos modelos toman en gran parte de su estructura la norma ISO 17799, la cual consta de diez secciones como se observa: (ver figura 46).

Figura 49 Norma ISO 17799 y los Modelos de Seguridad Informática



Fuente: Autor del Proyecto

Estos modelos presentan una metodología base caracterizada por lo general en las siguientes pautas:

- Normas de auditoría generalmente aceptadas
- Análisis de riesgos y controles
- Listas de chequeo y seguridad
- Herramientas automáticas comerciales.

A continuación se presentan los tópicos más relevantes de los principales modelos de seguridad informática:

ISO 17799 - BS 7799. Básicamente son una serie de controles que incluyen las "mejores prácticas" en seguridad de la información. Es un estándar genérico de seguridad reconocido internacionalmente. Fue desarrollado con la intención de servir como punto de referencia único para identificar los controles necesarios en la mayoría de las situaciones en que los sistemas de información se ven

involucrados en la industria y el comercio. Sirve para facilitar el comercio en un entorno confiable.

Existe como BS7799[25] desde 1995, aunque no se popularizo su aplicación debido a que fue criticado como simplista, poco flexible, además habían asuntos más urgentes que atender como el problema de fin de milenio llamado Y2K. Sin embargo en 1999 se publica una segunda versión revisada y empezaron a desarrollarse herramientas para facilitar su aplicación y las certificaciones comenzaron de manera formal. Este paso le permitió evolucionar muy rápido a un ISO, o sea un Estándar Internacional, provocando que muchas organizaciones declararan su intención de certificarse, especialmente instituciones financieras. Debido también, al inusitado interés que despertó el tema de la seguridad informática especialmente después de los eventos ocurridos el 11 de septiembre en Nueva York. Pero, ¿Porqué certificarse?- La respuesta pudiera ser por competitividad.-¿Qué pasaría si un competidor se certifica antes que nuestra organización? Sencillamente este hecho se convertiría en un factor diferenciador en el mercado, por lo tanto se aprecia la necesidad de certificación en cuestión de negocios, pero no solamente organizaciones de esta índole, sino también, cualquier organización que se respete tendrá que garantizar que la información de sus clientes se encuentra protegida y que no habrá fugas o pérdidas de información.

El ISO17799 esta organizado en 10 secciones principales, cada una cubre áreas o tópicos diferentes:

1. Planeación de la Continuidad del Negocio. Los objetivos son: contrarrestar las interrupciones de las actividades productivas críticas del negocio, como los desastres y fallas de gran magnitud.

2. Sistemas de Control de Acceso. Orientada a:

- Controlar el acceso a la información.
- Prevenir los accesos no autorizados a sistemas de información.
- Garantizar la protección de servicios de red.
- Prevenir los accesos no autorizados a los computadores.
- Detectar actividades no autorizadas.

[25]British Standards Institute (httpp://www.bsi-global.com).En la página BSI Catalogue (http://bsonline.techindex.co.uk) se puede buscar el estándar 7799. La versión actual del estándar tiene dos partes:
BS7799-1: 1999 Information Security Management Code of Practice for Information Security Management.
BS7799-2: 1999 Information Security Management Specification for Information Securtiy System.
El BSI ha implementado un esquema de certificación para el BS7799 el cual está disponible en http://www.c-cure.org/.

- Garantizar la seguridad de la información cuando se utilice cómputo móvil o remoto.

3. Desarrollo y Mantenimiento de Sistemas. Pretende asegurar que la seguridad del sistema esté construida dentro de la aplicación para prevenir perdidas, abusos, modificaciones de los datos. Debe proteger la:

- Confidencialidad
- Autenticidad e
- Integridad de la información.

Los proyectos informáticos y sus actividades de soporte deberán de ser conducidos de forma segura.

4. Seguridad Física y Ambiental. El objetivo de esta sección es prevenir el acceso no autorizado a las instalaciones para prevenir pérdida, robo, daño de los bienes y evitar la interrupción de las actividades productivas. Prevenir el robo de información y de los procesos de la empresa.

5. Cumplimiento. Pretende cumplir objetivos como:

- Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.

- Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.

- Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoria del proceso.

6. Seguridad del Personal. Orientada a: reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse que el personal este conciente de las amenazas a la información y sus implicaciones. Deberán de apoyar la política corporativa de seguridad en contra de accidentes y fallas.

7. Seguridad de la Organización. Los objetivos de esta sección son:

- Administrar la seguridad de la información dentro de la compañía.

- Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos accesados por terceros, (proveedores, clientes, etc.)

- Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros (outsourcing)

8. Administración de las Operaciones y equipo de Cómputo. Orientada a cumplir objetivos como:

- Asegurar la correcta operación de las instalaciones de procesamiento.
- Minimizar el riesgo de fallas en el sistema.
- Proteger la integridad del software y la información

- Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.

- Asegurar la protección de la información en la red y de la infraestructura que la soporta.

- Prevenir el daño a los activos y procesos críticos del negocio.

- Prevenir la perdida, modificación o mal uso de la información intercambiada entre empresas.

9. Clasificación y Control de Activos. Los objetivos son mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

10. Políticas de Seguridad. Objetivo: Proveer la directriz y el soporte de la Dirección General de la empresa para la seguridad de la información.

Se puede concluir que alinearse con la norma ISO17799 no es una tarea fácil, incluso para las organizaciones con más conciencia en la seguridad, por esto es recomendable que sea implementada paso a paso, donde el punto de partida consiste en realizar un análisis de la posición y situación de la organización, seguido de una identificación de los cambios necesarios para ajustarse a ISO 17799. Luego el proceso de planeamiento e implementación se emprenderá metódicamente y abierto al cambio.

COBIT. El incremento masivo en el uso de las computadoras y el desarrollo de aplicaciones cada vez más sofisticadas han instado la necesidad de adoptar diferentes técnicas de auditoría para hacer frente a estos cambios. Dentro de estas se plantea el empleo de un nuevo modelo llamado COBIT cuyas siglas significan: Objetivos de Control para la Información y Tecnologías afines.

El Modelo COBIT supone un enfoque distinto y actual del sistema por cuanto lo mira en su ámbito global, formado por procesos manuales e informáticos. El

Modelo COBIT supone un aporte de máximo interés para los auditores ya que incorpora aspectos de gestión de la calidad total, reingeniería de empresas e integra los dos modelos de control: los orientados a las Tecnologías de Información y los orientados a los Objetivos Empresariales. Por lo tanto esta orientado a ayudar al entendimiento y a la administración de riesgos asociados con tecnologías de información y con tecnologías relacionadas.

El Modelo COBIT permite verificar la debida correspondencia entre los objetivos de una entidad y el empleo de las tecnologías de Información, por cuanto está orientado a los objetivos, pudiendo verificar incongruencias entre el objetivo fundamental del auditado y el empleo de la técnica, ineficiencia y falta de efectividad en las operaciones materializados en considerables pérdidas económicas, insuficiente gestión de los equipos de cómputo cuya depreciación contable no se corresponde con el ritmo de explotación que encierra el recurso, detección de formas de fraude que ponen en peligro la consecución de los objetivos fundamentales trazados por la entidad por la falta de seguridad, auditabilidad y confiabilidad en los procesos.

COBIT no intentó reinventar la rueda, se utilizaron las definiciones de COSO (Committee of Sponsoring Organisations of the Treadway Commission. Internal Control-Integrated Framework) para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, la confiabilidad de información fue ampliada para incluir toda la información no sólo información financiera. Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, los cuales son utilizados a nivel mundial para describir los requerimientos de seguridad.

Dominios. Contemplan la totalidad de los procesos típicos de la función de tecnología de prácticamente cualquier organización de negocios, agrupados en:

- Planificación y Organización
- Adquisición e Implementación
- Entrega y Soporte
- Monitoreo

Los dominios están constituidos genéricamente por treinta y cuatro procesos distribuidos en cada uno de los cuatro anteriormente mencionados así:

Planificación y Organización. Dominio que abarca la estrategia y las tácticas. Se refiere a la identificación de la forma en que la tecnología de información puede

contribuir de la mejor manera al logro de los objetivos del negocio. Conjuntamente, la adquisición de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. También buscará la infraestructura tecnológica apropiada para la organización.

Los once procesos directamente relacionados con el dominio de planificación y organización son:

- Definición de un plan estratégico de tecnologías de información (TI).
- Definición de la arquitectura de la información.
- Determinación de la dirección tecnológica.
- Definición de la organización y las relaciones de tecnologías de información (TI).
- Administración de la inversión en tecnologías de información (TI).
- Comunicación de los objetivos y directivas de la gerencia.
- Administración de los recursos humanos.
- Garantía del cumplimiento de los requisitos externos.
- Evaluación de riesgos.
- Administración de proyectos.
- Administración de calidad.

Adquisición e Implementación. Las soluciones de tecnologías de información (TI) deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes. Los procesos que conforman este dominio son:

- Identificar soluciones de automatización
- Adquirir y mantener software de aplicación
- Adquirir y mantener la arquitectura tecnológica
- Desarrollar y mantener procedimientos

- Instalar y acreditar sistemas de información

- Administrar cambios

Entrega y Soporte. Dominio relacionado con la entrega de los servicios requeridos, que abarca desde operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

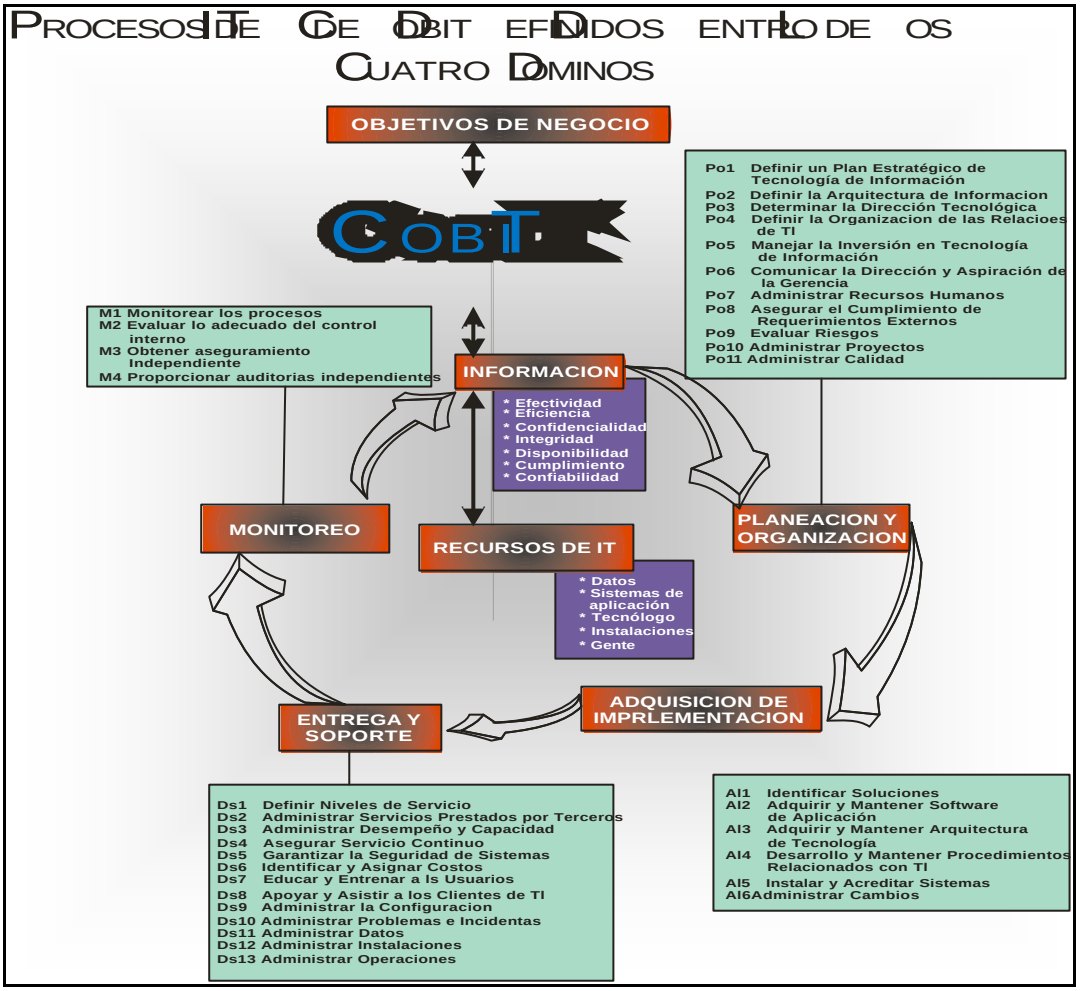
- Definir niveles de servicio
- Administrar servicios de terceros
- Administrar desempeño y capacidad
- Asegurar continuidad de servicio
- Garantizar la seguridad de sistemas
- Identificar y asignar costos
- Educar y capacitar a usuarios
- Apoyar y orientar a clientes
- Administrar la configuración
- Administrar problemas e incidentes
- Administrar la información
- Administrar las instalaciones
- Administrar la operación

Monitoreo. Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

- Monitorear el proceso
- Evaluar lo adecuado del control interno
- Obtener aseguramiento independiente
- Obtener aseguramiento independiente
- Proporcionar auditoría independiente

El siguiente diagrama ilustra el modelo:

Figura 50 Modelo de Procesos COBIT



Fuente: IZQUIERDO DUARTE,F (2002). *Estándar de Controles y Auditoría de Tecnología Informática COBIT*.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, para esto y orientando el modelo COBIT hacia la seguridad informática dice que se deben tener en cuenta las siguientes pautas:

- Producir políticas de seguridad.
- Diseñar defensas de seguridad.
- Ejecutar un monitoreo activo.

- Ejecutar pruebas de intrusión.

- Gestión de la seguridad.

MAGERIT. Modelo Español cuyas siglas significan: Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas, cuya utilización promueve, como respuesta a la dependencia creciente de éstas (y en general de toda la sociedad) de las Tecnologías de la Información. La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la:

- Autenticación

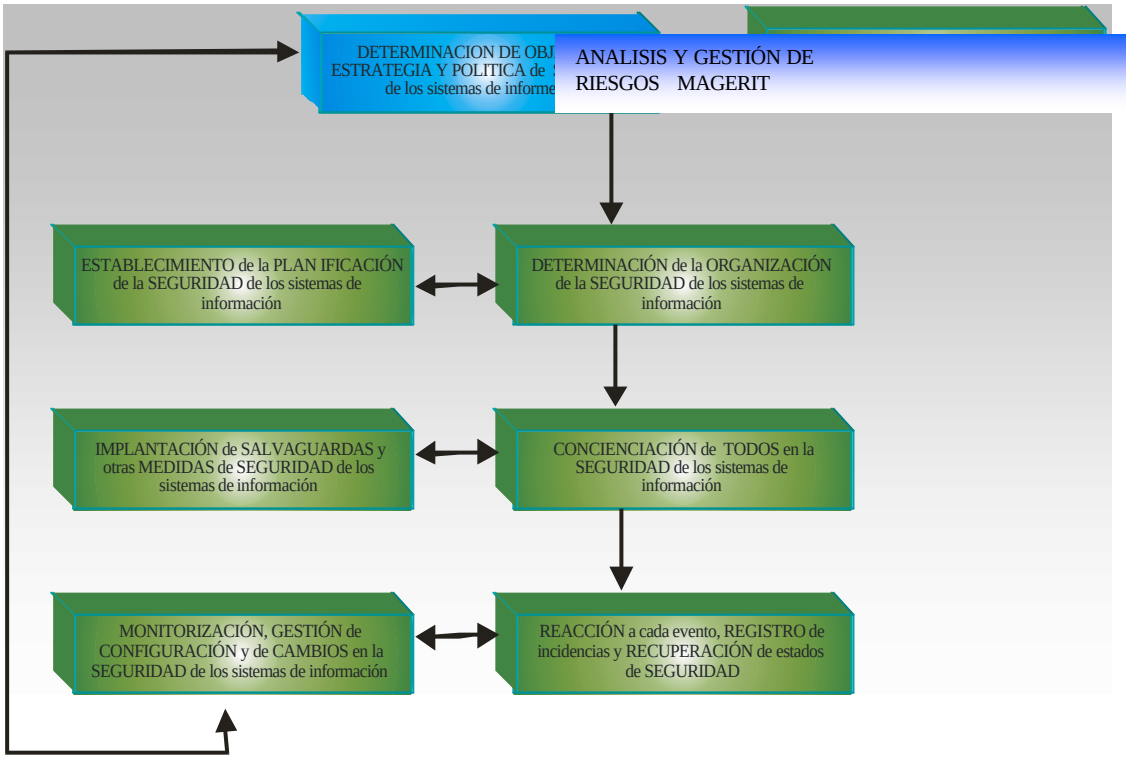
- Confidencialidad

- Integridad y

- Disponibilidad de los sistemas de información (conceptos estos que se definen con precisión en la Guía de Procedimientos) y generen confianza cuando se utilicen tales.

El Análisis y Gestión de Riesgos es el ‘corazón' de toda actuación organizada en materia de seguridad y, por tanto, de la gestión global de la seguridad. Influye en las fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento). A continuación se ilustra gráficamente este modelo:

Figura 51. Fases y estrategias MAGERIT



Fuente: Metodología de Análisis y Gestión de Riesgos MAGERIT. Versión 1.0

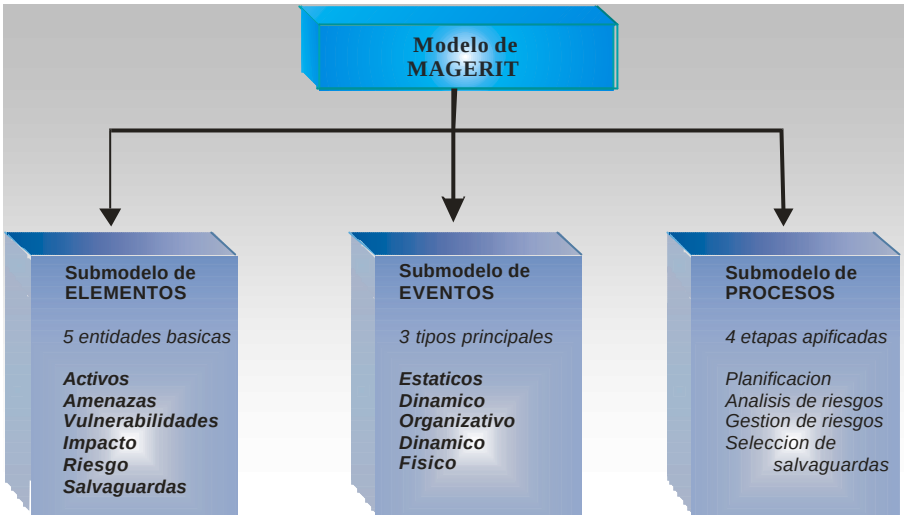
Objetivos de MAGERIT. El método MAGERIT tiene un objetivo inmediato doble:

- Estudiar los riesgos que soporta un determinado sistema de información (SI) y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la acepción habitual del término.

- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

- Como objetivo a más largo plazo, MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información.

Figura 52. Submodelos Componentes de MAGERIT



Fuente: Metodología de Análisis y Gestión de Riesgos MAGERIT. Versión 1.0

3.3 MODELO DE SEGURIDAD INFORMÁTICA PROPUESTO

Como se puede observar en la figura 52, el modelo propuesto está compuesto por una serie de políticas, estándares y procedimientos, los cuales son a menudo bastantes confusos de entender si de seguridad informática se trata. La figura 50 pretende aclarar las diferencias entre estos conceptos:

Figura 53. Políticas, Estándares y Procedimientos de Seguridad Informática

Fuente: Autor del Proyecto.

- La política de seguridad explica con documentación el **por qué** una organización protege su información.

- Los estándares de la organización revelan con documentación lo **qué** la organización quiere hacer para implementar y administrar la seguridad de su información.

- Los procedimientos dicen con documentación exactamente **cómo** la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior.

Políticas (Según la RFC 1244). No es una descripción técnica de mecanismos ni una expresión legal que involucra sanciones a conductas de los empleados, es más bien una descripción de lo que se desea proteger y el por qué de ello. Las políticas de seguridad surgen como una herramienta organizacional para concientizar a cada uno de los miembros de la organización sobre la importancia y sensibilidad de la información y servicios críticos. Estas permiten a la organización desarrollarse y mantenerse en su sector de negocios. En el caso de la UIS, las políticas de seguridad determinarían lo que esta organización considera valioso, las medidas a tomar, permitiendo además:

- Aclarar que se está protegiendo
- Establecer la responsabilidad de la protección
- Sentar las bases para resolver conflictos posteriores.

Las políticas se establecen sobre la plataforma tecnológica de la organización, que en este caso es una Intranet con diversa complejidad informática, dividida en tres niveles:

- Nivel lógico: el cual consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permita acceder a ellos a las personas autorizadas para hacerlo.

- El nivel físico: orientado a la protección activos físicos informáticos de la empresa.

- El nivel de talento humano: relacionado con la concientización de una cultura de seguridad en la organización.

Elementos de una Política de Seguridad Informática. Una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las políticas de seguridad deben considerar principalmente los siguientes elementos:

- Alcance de las políticas

- Objetivos de la Política y descripción clara de los elementos involucrados en su definición.

- Responsabilidad por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.

- Definición de violaciones y sanciones por no cumplir con las políticas

Las políticas de seguridad informática también deben:

- Ofrecer explicaciones comprensibles sobre porque deben tomarse ciertas decisiones y explicar la importancia de los recursos

- Deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones

- Deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos, claro sin sacrificar su precisión

- Deben seguir un proceso de actualización periódica sujeto a los cambios de las organizaciones relevantes, como son el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocio, etc.

Parámetros para establecer políticas de seguridad: Se deben considerar los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Identificar quien tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los archivos críticos de su área.

- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.

- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer mecanismos de seguridad que respondan a las políticas trazadas.

Razones que impiden la Aplicación de las políticas de seguridad informática:

- Convencer a los directivos de las necesidades de estas políticas

- Los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los gerentes de informática o los especialistas de seguridad que llevan a pensamientos como: “más dinero para juguetes del departamento de sistemas”.

- Ante esta situación los encargados de seguridad deben constatar que las personas entienden los asuntos importantes de la seguridad.

- Si se quieren que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a la misión, visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía

- Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión del negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Estándares. Los estándares de seguridad de la información constan de documentos múltiples que se aplican a todas las áreas de la empresa que utilizan la información, abarcando controles de seguridad físicos, administrativos y lógicos (técnicos), que son diseñados para proteger la información. No deben ser desarrollados de manera aislada. Algunas consideraciones claves a tener en cuenta para el desarrollo de estándares son:

- Cualquier estándar de seguridad de la información debe respaldar los objetivos comerciales de la organización y las normas y reglamentaciones que aplican a la empresa y sus operaciones y que son afines con otras políticas organizacionales.

- Los Estándares de Seguridad de la Información se deben diseñar para proteger la información y para que los usuarios de la misma realicen sus funciones normales sin tener que hacer esfuerzos irrazonables para acceder a la información que necesitan para ser productivos.

- Los Estándares de Seguridad de la Información deben respaldar únicamente los requerimientos especificados en la Política de Seguridad de la Información. Si se exige el cumplimiento de la Política de Seguridad de la Información, también se exigirá el cumplimiento de los Estándares de Seguridad de la Información relacionados.

- Para que los Estándares de Seguridad de la Información sean efectivos y utilizables, los dueños de la empresa y los expertos técnicos deben trabajar mancomunadamente para producir los documentos. Esto es importante porque el siguiente nivel de documentación - los procedimientos - deben cumplir totalmente con los requerimientos especificados en estos estándares y respaldarlos.

- La creación de los Estándares de Seguridad de la Información es una tarea tanto comercial como técnica que requiere de la interacción humana para garantizar que los resultados finales satisfagan las necesidades de la empresa y sean aceptados como parte normal de las operaciones de la empresa por parte de las personas para quienes aplican los estándares.

- Lo más importante es que todo Estándar de Seguridad de la Información debe cumplir con los requerimientos de seguridad exigidos por la Política de Seguridad de la Información.

Procedimientos. Explican con documentación exactamente **cómo** la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior. Los procedimientos de seguridad de la información establecen de manera detallada las operaciones que deben realizarse para satisfacer los requerimientos especificados en el Estándar que se aplica a una actividad determinada, proceso de seguridad o protección a un recurso de la información.
Ni la política ni los estándares relacionados definen cómo se deben implementar y administrar los controles de la seguridad, ya que es función de los procedimientos de seguridad de la información; son documentos de uso diario, la "hoja de ruta" o guía del personal de redes y sistemas, y el departamento de seguridad de la información. Si los procedimientos están adecuadamente trazados para los estándares, la administración del cumplimiento de los requerimientos de seguridad

es simplemente cuestión de asegurar que se sigan detalladamente los procedimientos.

Además de desarrollar los procedimientos para implementar los requerimientos especificados en los estándares, usted debe desarrollar un proceso para evaluar y permitir excepciones. Estas excepciones (bajo circunstancias muy controladas) permiten el incumplimiento de procedimientos específicos. Es imperativo que usted limite estrictamente el tiempo y alcance de dicho proceso para evitar abusos.

Administración de los cambios a los Procedimientos de Seguridad de la Información. Se requieren significativamente más documentos de procedimiento que la cantidad total de documentos de seguridad de la información de nivel superior (la política y sus estándares relacionados). Los procedimientos están orientados por tareas y cualquier estándar requerirá usualmente que se realicen muchas actividades para lograr el cumplimiento del estándar.

Es típico que los documentos de la política y los estándares no se modifiquen con frecuencia después de su aceptación inicial. Sin embargo, los documentos de procedimiento de seguridad de la información suelen ser alterados a menudo en entornos computacionales, operativos y comerciales, por lo tanto es urgente mantener buenos procesos de administración de cambio de los documentos para estos procedimientos. De hecho, el procedimiento de administración de cambio de los documentos debe ser el primer procedimiento que usted documente.

Cada procedimiento debe utilizar un formato y presentación estándar, para que los usuarios que necesiten cumplir con los múltiples procedimientos, no se confundan con los múltiples estilos y presentaciones. Lo ideal es que los procedimientos estén al alcance de los usuarios tanto en formato escrito como electrónico.

Obviamente algunos procedimientos pueden contener información sensible corporativa, para lo cual la accesibilidad debe estar muy controlada. En estos casos, no sería prudente publicar estos documentos en un sitio Web de intranet que no controle el acceso de los empleados (lo que probablemente será prohibido por uno de los estándares).

Elementos recomendados de un Procedimiento. A continuación se muestra el esquema[26] o plantilla de un procedimiento:

---

[26] Stuart Broderick, PhD, está encargado del desarrollo de los Servicios de Seguridad de Symantec alrededor del mundo. Los Servicios de Seguridad de Symantec ofrecen soluciones para la seguridad de la información que incorporan lo mejor de la tecnología, prácticas eficientes de seguridad y pericia y recursos globales que permitan el éxito de las compañías en un mundo electrónico. Dr. Broderick ha realizado múltiples consultorías senior en seguridad y desarrollo empresarial para firmas de alta tecnología en Inglaterra y Estados Unidos. Tiene 19 años de

- Propósito del procedimiento
  - Qué estándar cumple
  - Cuál es el objetivo del procedimiento
- Alcance del procedimiento
  - A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento
  - Qué función se espera que este proceso ejecute
  - Los conocimientos previos que se necesitan tener para ejecutar el proceso
- Definición del proceso
  - Introducción al proceso
    - Descripción de lo qué el proceso hace
  - Descripción detallada de:
    - Cómo se ejecutará el proceso
    - Cuándo se ejecutará el proceso
    - Lo que se espera que suceda durante la ejecución del proceso
    - Lo que no se espera que suceda
    - Las acciones que se tomarán si ocurre un hecho imprevisto
    - Qué criterios indican la ejecución exitosa del proceso
    - Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará
    - Las interacciones requeridas o esperadas de otros procesos
- Listas de los procesos
- Problemas de los procesos
  - Qué se hará si se presenta un problema en el proceso
    - Error de proceso
    - Excepción del proceso por no aplicabilidad

Aspectos esenciales para el desarrollo de procedimientos exitosos
Los procedimientos deben estar escritos en lenguaje sencillo para que cualquier usuario pueda entenderlo. Si necesita utilizar jerga o siglas, adjunte un glosario al procedimiento y desarrolle un Estándar del glosario con todos los términos utilizados en el paquete de documentación de la seguridad.

La elaboración de los Procedimientos de seguridad de la información es una tarea que es desarrollada por o con el personal que ejecutará el procedimiento. Muchas organizaciones han descubierto que las personas que no están involucradas en el desarrollo del proceso por lo general no demuestran "sentido de propiedad" por el

---

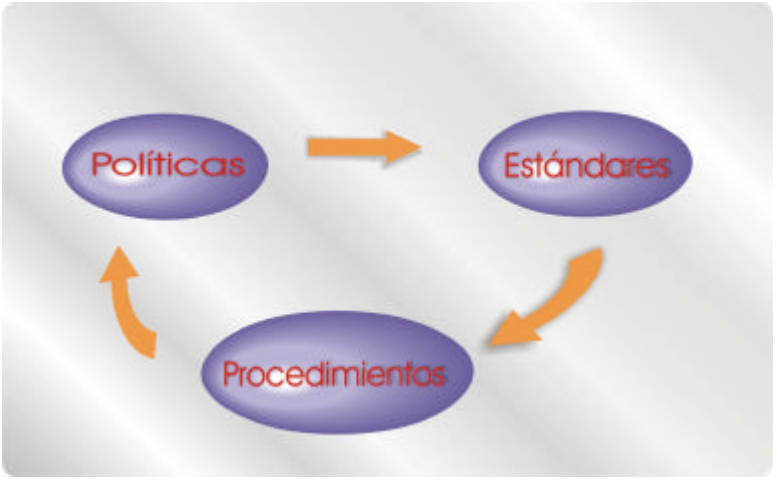
experiencia en la creación de programas personalizados de capacitación de servicio al cliente y en el desarrollo y despliegue de programas clave de administración, implementaciones, políticas, procedimientos y prácticas para la seguridad.

proceso y creen que su conocimiento sobre la forma cómo operan los sistemas, no es valioso.

Por consiguiente, este personal está dispuesto a ignorar el proceso y adoptar una actitud de "Yo se más que eso" o "Siempre lo hemos hecho de esta manera", lo que no augura un buen resultado para los departamentos, a los que se les puede hacer auditorias para verificar si cumplen con los procesos aplicables. En el caso de una auditoría, el cumplimiento con los procesos es decisivo y no quien escribió el proceso y si es percibido como correcto o no.

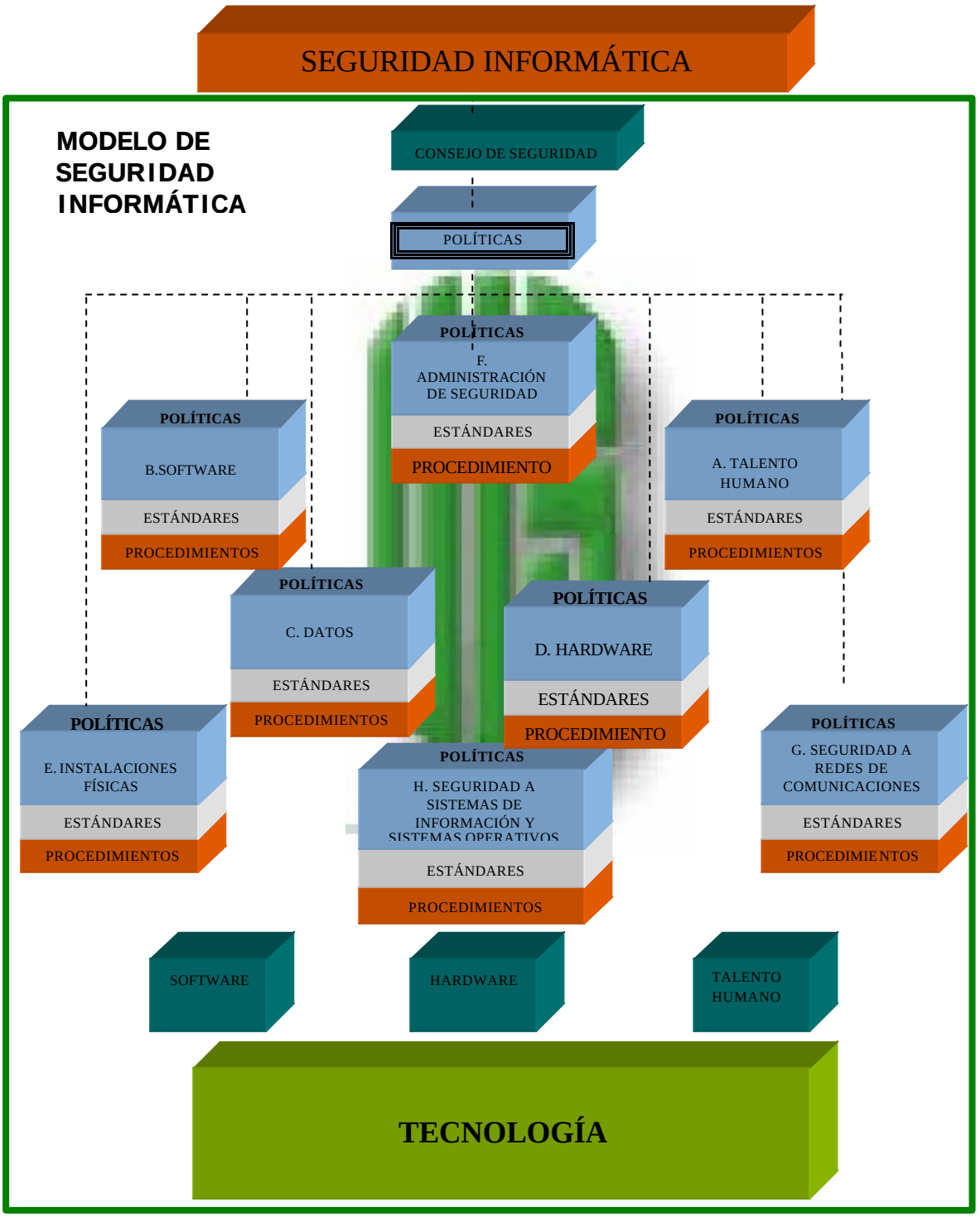
3.3.1 Dinámica del modelo de seguridad informática propuesto. Hasta el momento se indagó acerca de la norma base o referencia de los principales modelos de seguridad informática del mundo, es decir la norma ISO 17799, la cual está anclada a unas estructuras claves que le dan soporte al modelo de seguridad y son las políticas, estándares y procedimientos, los cuales además de las características expuestas anteriormente deben actuar cíclicamente y rotativamente en la organización en forma continua, igual de dinámico y cambiante como es el mundo de las amenazas y vulnerabilidades informáticas. En la cual la política (Ver figura 28)genera una serie de estándares, los cuales para cumplirlos obligan a tomar medidas efectivas, surgiendo así los procedimientos, luego se evalúa el funcionamiento de la política: si es efectiva, permanece, pero si por el contrario no cumple los objetivos, debe mejorar, obligando a comenzar de nuevo el ciclo, donde es muy importante la estrategia de concientización acerca de la importancia y conveniencia de la seguridad por parte del personal de la universidad.

Figura 54. Dinámica del Modelo de Seguridad Informática Propuesto



Fuente: Autor del Proyecto

Figura 55. Modelo de Seguridad Informática Propuesto



Fuente: Autor del proyecto

3.3.2 Organización de la UIS. Las directivas de la UIS debe ser conscientes que existen facilidades para acceder a los Recursos Informáticos y Activos de Información e incluso manipularlos, sin motivos basados en el objeto de la universidad, es decir sin autorización.

3.3.3 Consideraciones Organizativas. La UIS tiene una organización jerárquica en forma piramidal, cuya parte superior está ocupada por las Directivas. Entre la parte superior y la base existen varios niveles intermedios.

Un departamento, o grupo de departamentos homogéneos, forma lo que llamaremos una Función (ej: División Financiera, Biblioteca, Facultades, División de Servicios de Información, Finanzas, Administración, Recursos Humanos, etc). Entre ellas, sobresalen la División de Servicios de Información, que es la encargada de gestionar los Recursos Informáticos y los Activos de Información de las restantes funciones de la universidad.

En la medida que cada Función y el objeto o razón social de la UIS dependa de la información, se hace más urgente la necesidad de protección y cada vez tendrá que ser más sofisticada.

3.3.4 Estructura del Consejo de Seguridad de la UIS. Se debe tener en cuenta que, dependiendo del tamaño de la empresa como también de los recursos con que cuente, algunos puestos no siempre serán cubiertos y que varios puestos pueden ser desempeñados por la misma persona. Este comité se puede estructurar así:

1. En la Dirección de la UIS

Comité de Dirección: conformado por los Directores Funcionales que pudieran ser los mismos Directores o Coordinadores de cada Escuela, los cuales ahora deben preocuparse por la seguridad informática de cada Escuela y tendrían como funciones las siguientes:

- Servir como medio para recoger las inquietudes y problemas que surjan en cada Escuela relacionados con la seguridad informática.

- Velar por el funcionamiento adecuado de los equipos y la red de datos de su respectiva Escuela.

- Servir como organismo de control y certificación de las actividades efectuadas por los coordinadores funcionales en su respectiva Escuela.

- Asistir, transmitir y coordinar inquietudes y posibles soluciones de seguridad informática en concertación con las directivas del Consejo de seguridad.

- Ayudar a propiciar mediante acciones, publicidad entre otras una cultura de concientización respecto a la seguridad a la información.

- Velar por el estricto cumplimiento tanto de las políticas como de los estándares y procedimientos de seguridad implantados por la UIS.

Ejecutivo de Seguridad Informática: Generalmente el Jefe de la División de Servicios de Información, dependiendo del más alto nivel directivo de la UIS, el cual ahora también tendrá funciones relacionadas con la seguridad informática como:

- Gestionar la consecución de partidas o recursos necesarios para el funcionamiento del Consejo de Seguridad Informática ante las directivas de la UIS.

- Buscar el respaldo por parte de las directivas de la UIS a las diversas políticas, estándares y procedimientos que sean necesarios para reforzar la seguridad.

Experto en Legislación Informática. Tendrá a su cargo todo lo relacionado con la parte jurídica de la seguridad informática como:

- Asesorar en los procesos jurídicos que puedan surgir en contra del atacante informático.

- Orientar las sanciones legales que se pueden tomar contra los funcionarios que incumplan las políticas de seguridad de la organización.

- Orientar todos los aspectos legales acerca de los derechos de autor, software legal entre otros.

Comité de Seguridad Informática: Conformado por el Director de Seguridad Informática, el Administrador Central de Seguridad Informática, el Coordinador de Seguridad Informática ,el Administrador de Usuarios y Accesos y por lo general un representante de los coordinadores funcionales. Este comité tendrá entre sus principales atribuciones las siguientes:

- Analizar los informes mensuales reportados por el Administrador Central de seguridad informática, el Coordinador de Seguridad informática, el Administrador de Usuarios y Accesos.

- Generar las políticas estándares y procedimientos de seguridad informática necesarias para fortalecer la seguridad informática de la UIS.

- Aconsejar los respectivos cambios y explicar el por qué la necesidad de modificar ya sea la política, el estándar y el procedimiento.

- Analizar los informes mensuales reportados por el Administrador Central de seguridad informática, el Coordinador de Seguridad informática, el Administrador de Usuarios y Accesos.

- Recomendar la compra de equipos y herramientas de seguridad informática.

2. En la Función de la División de Servicios de Información:

Jefe de la División de Servicios de Información. Tiene a su cargo esta división con todas las responsabilidades que implica el brindar los servicios de información en forma ágil rápida y oportuna, pero ahora también segura, para esto su labor estará enfocada a la gestión de los recursos necesarios para fortalecer la seguridad como también el de conseguir el apoyo a las políticas necesarias para el mismo.

Director de Seguridad Informática. Dependerá del Jefe de la División de Servicios de Información. Dentro de sus principales funciones:

- Implantar las políticas aprobadas por la universidad, apoyado en los estándares y procedimientos.

- Evaluar los resultados de la implantación de las políticas aprobadas.

- Impulsar proyectos relacionados con la seguridad informática que sean necesarios para el Consejo de Seguridad de la UIS.

- Controlar que el personal a cargo está actuando efectivamente ante las amenazas encontradas.

El director de seguridad informática tendrá a cargo los siguientes funcionarios:

El Coordinador de Seguridad Informática. Es el líder de los coordinadores funcionales de seguridad informática, debe contar con un gran dominio de la mayor parte de los frentes de la seguridad informática: sistemas operativos, redes, antivirus, herramientas de seguridad las diferentes áreas de la seguridad informática, todo esto orientado al hacer y su principal función será:

- Controlar, vigilar y hacer que las medidas necesarias para cumplir con las políticas, estándares y procedimientos se cumplan. Es decir sean efectuadas por los funcionarios a su cargo que serían los coordinadores funcionales.

El Administrador Central de Seguridad Informática. Bajo su responsabilidad estará a cargo el manejo y supervisión de tecnologías de seguridad. Cumplirá funciones como:

- Reemplazar al director de seguridad cuando sea necesario, por lo tanto debe saber conocer todas las funciones y conocer todas las claves de todos los sistemas de seguridad que maneje la universidad.

- Supervisar las diferentes tecnologías de seguridad, como por ejemplo el control de contenidos Websense, el firewalll de la universidad entre otras.

El administrador de Usuarios y Accesos. Encargado de organizar los usuarios y sus respectivos accesos, por lo tanto tendrá funciones como:

- Llevar a la realidad mediante el cumplimiento de las políticas, estándares y procedimientos todo lo relacionado respecto a Usuarios y Accesos.

- Asignar y diseñar procedimientos adecuados para los nombres de usuarios y escogencia de una buena clave.

- Propiciar una cultura organizacional para la protección de los nombres y usuarios

- Implementar las herramientas necesarias para asegurar los nombres y claves de usuarios.

3. En las Restantes Funciones de la UIS

Coordinador Funcional de Seguridad Informática. Dependiendo directamente tanto del Coordinador de seguridad Informática como del Director de la Función correspondiente (Directores de Escuelas). Su función principal radica en el hacer, ya que sería la parte operativa del Consejo de Seguridad Informática de la UIS. Por lo tanto unificando su principal función sería:

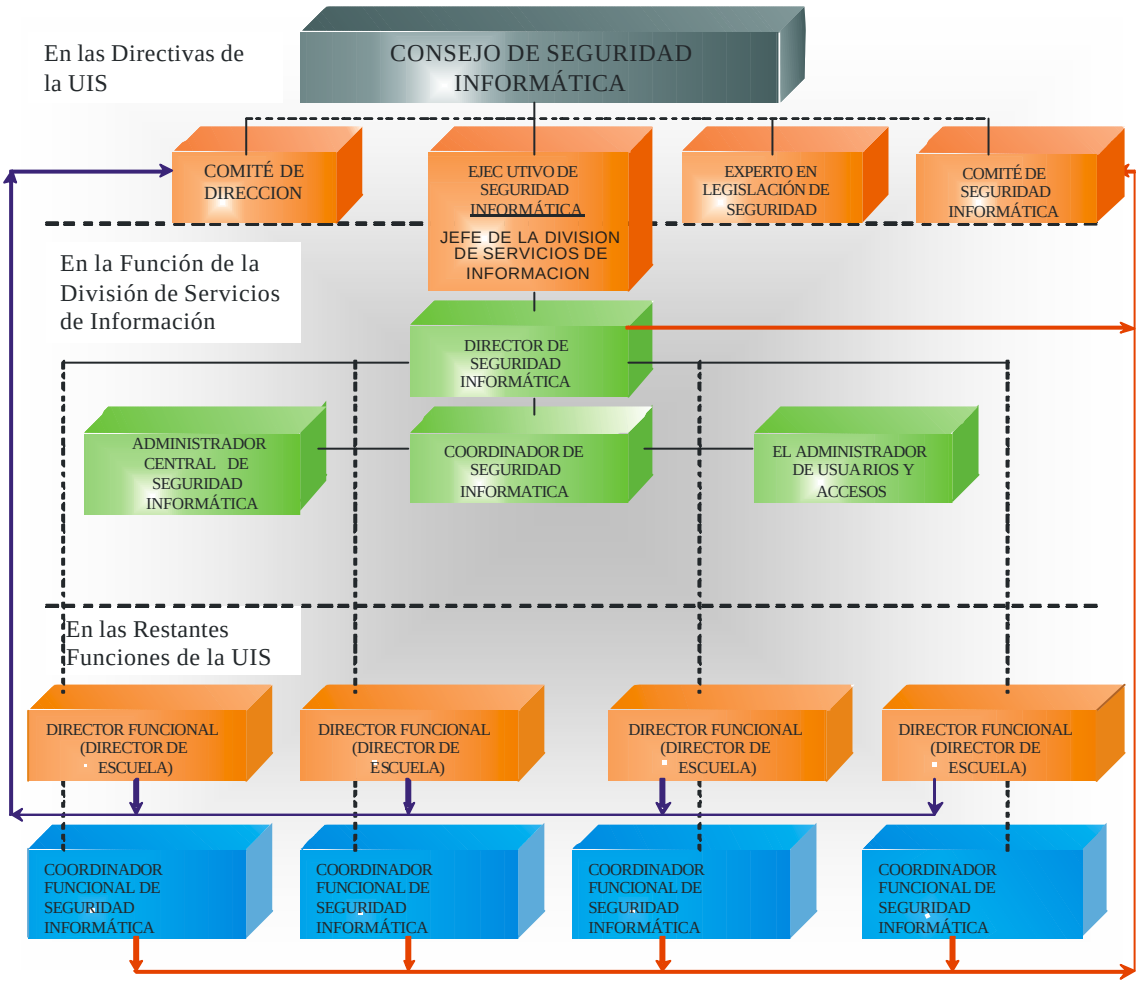
- Solucionar mediante maniobras técnicas los diversos inconvenientes de amenaza informática que se puedan presentar en los diversos sitios de la UIS.

- Como su labor radica en el hacer, deben colaborar con el Consejo de Seguridad para establecer los mejores procedimientos de seguridad informática a seguir ante las diversas eventualidades que afrontan. Este personal debe ser capacitado por **Especialistas Informáticos.** Que asesorarán a los coordinadores, que pueden ser los docentes de Seguridad Informática de la Especialización en Telecomunicaciones y materias que se dicten en la Escuela de Ingenierías de Sistemas e Informática de la UIS.

Es conveniente resaltar que el Consejo De Seguridad Informática puede requerir **Soporte de Especialistas en Seguridad Informática.** En lo posible, este soporte debe ser dado por un asesor interno, aunque puede ser habitual el contratar

asesores ajenos a la Universidad. Estos especialistas deben poder asesorar sobre todos, y cada uno de los aspectos de la Seguridad Informática. Tienen que evaluar el nivel de implantación de las Políticas y el nivel de cumplimiento de los procedimientos establecidos. Tienen que poder analizar los riesgos, definiendo las posibles amenazas, detectando las vulnerabilidades existentes y determinando las medidas a tomar para su eliminación o reducción. Los especialistas deben ser consultados lo más rápidamente posible cuando se sospechen incidentes o debilidades de Seguridad, para que se establezcan planes de actuación y métodos de aislamiento e investigación del problema.

Figura 56. Estructura Consejo de Seguridad UIS



Fuente: Autor del Proyecto.

3.4 DEFINICIÓN DE POLÍTICAS Y ESTÁNDARES FORMALES DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

A. TALENTO HUMANO. Los empleados y la seguridad de la información.

La responsabilidad por la seguridad de la información no es únicamente de las áreas de seguridad informática, es una obligación de cada funcionario.

1. Respecto a los códigos de identificación y palabras claves(passwords):

1.1 Las palabras claves o los mecanismos de acceso a los recursos informáticos que le sean entregados a los funcionarios son responsabilidad exclusiva de cada uno de ellos, no deben ser divulgados a ninguna persona, con excepción de que sea un requerimiento legal o sea un procedimiento de revisión de claves que lleve a cabo el consejo de seguridad de la UIS.

1.2 Cada usuario es responsable de todas las actividades que realice con su código de identificación de usuario y sus claves personales. Los códigos de identificación y las claves personales son de uso personal e intransferibles.

2. Control de la información.

2.1 Los usuarios deben informar inmediatamente al área encargada dentro de la universidad cualquier vulnerabilidad detectada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

2.2 No es permitido a los usuarios instalar software en sus equipos o en servidores sin las respectivas autorizaciones.

2.3 No es permitido a los usuarios intentar sobrepasar los controles de los sistemas, explorar los computadores y redes de la universidad en busca de archivos de otros sin su respectiva autorización o introducir intencionalmente software que pueda causar daño o impedir el normal funcionamiento de los sistemas de la universidad.

2.4 Los funcionarios de la universidad no deben suministrar información a ningún ente externo sin la respectiva autorización, esto incluye los controles del sistema de información y su respectiva información.

2.5 Ningún funcionario debe consultar, modificar, copiar, distribuir o destruir los archivos de la universidad sin los permisos respectivos.

2.6 La universidad se reserva el derecho de revisar e implantar normas tendientes a controlar las actividades que realizan los funcionarios en sus horas laborales. (Orientado especialmente al uso del correo electrónico, chat y otros servicios que puedan distraer a los funcionarios de sus funciones).

2.7 Todo empleado de la universidad que use recursos de los sistemas tiene la enorme responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad y auditabilidad de la información que maneje, especialmente con la información que ha sido clasificada como crítica.

3. Otros Usos:

3.1 Los computadores, sistemas y otros equipos deben usarse exclusivamente para actividades propias de la universidad, por tanto los usuarios no deben utilizar ningún equipo para asuntos personales, a menos de que exista un permiso respectivo que evalúe el riesgo informático.

3.2 La universidad debe definir un código de ética para la seguridad informática, este debe incluir tópicos relacionados con la seguridad informática y de datos.

B. SOFTWARE. Administración, Operación y Control del Software Institucional. Cualquier empleado de la universidad que desempeñe funciones y responsabilidades relacionadas con software institucional deberá seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje:

1. Administración del Software:

1.1 La universidad debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Respecto a las licencias, estas se almacenarán bajo adecuados niveles de seguridad e incluidas en un sistema de administración, que efectúe continuos muestreos para garantizar la consistencia de la información almacenada. Cualquier software y documentación que pertenezca a la universidad incluirá avisos derechos de autor y propiedad intelectual.

1.2 Todas las aplicaciones deberán clasificarsen en una de las siguientes categorías: **Misión Crítica, Prioritaria y Requerida.** Respecto a las aplicaciones de misión crítica y prioritaria deberá existir una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alterno y muy seguro.

1.3 Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y

seguridad. Los programas que se encuentren en el ambiente de producción de la Universidad, se modificarán únicamente por personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, se considerarán planes de contingencia y recuperación.

1.4 La universidad deberá definir procedimientos que permitan un adecuado manejo de requerimientos de cada aplicación, manejo de versiones y auditabilidad (que permita establecer quién,cuándo y qué cambio se realizó al software.

1.5 La universidad deberá generar procedimientos para la generación de copias de respaldo, asegurar la correspondencia entre fuentes y ejecutables y almacenar adecuadamente toda la documentación relacionada con cada una de las diferentes aplicaciones utilizadas.

1.6 La universidad establecerá políticas que permitan prohibir o restringir la instalación de software adquirido por sus empleados en equipos propios del alma mater.

2. Respecto a la Adquisición del Software.

2.1 La universidad deberá estipular una metodología formal para el proceso de adquisición de software de misión crítica o prioritaria a través de terceros que incluirá un contrato con claúsulas básicas para la protección de la información y del software, así como para la documentación y los respaldos, que permitan proteger los intereses institucionales frente a las claúsulas ofrecidas por el vendedor.

2.2 El software contará con procedimientos de acceso controlado que permita al propietario del recurso restringir el acceso al mismo; el software protegerá los objetos con el fin de que los procesos y los usuarios no los puedan acceder sin los debidos permisos.; cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que el sistema se lo permita. El software auditará los eventos en el sistema relacionados con seguridad. Para cumplir con lo anterior es necesario que el software incluya el plan de cuentas, el plan de auditoria y el cierre de puertas traseras.

2.3 Al adquirirse una licencia de uso de software, a través de un proveedor o la contratación es de software a la medida, el vendedor deberá depositar en custodia en una empresa especializada una copia del software adquirido y su documentación técnica respectiva y sus correspondientes actualizaciones. También dejará una autorización por escrito para que la universidad los pueda retirar en caso de que el vendedor deje de existir en el mercado.

2.4 Con el fin de disminuir los riesgos acerca de información administrada en aplicaciones adquiridas a través de terceros o las desarrolladas en casa, el

documento de especificaciones incluirá un capítulo relativo a la seguridad informática.

3. Parametrización:

Con el fin de asegurar la integridad de la información, la función de parametrización estará a cargo de un equipo interdisciplinario. En el caso de aplicaciones de misión crítica y prioritaria, el grupo interdisciplinario representará a los diferentes usuarios e incluirá al proveedor. Para pasar el software al ambiente de pruebas, el documento final de parametrización del software contará previamente con las aprobaciones correspondientes al interior de la universidad.

4. Desarrollo de Software:

4.1 La Universidad deberá contar con una metodología formal para el desarrollo de software de los sistemas de información de misión crítica y prioritaria, desarrollos rápidos del mismo y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas procedimientos, controles y otras convenciones estándares aplicables en el desarrollo de sistemas. Respecto a los controles desarrollados internamente estos deberán ser como mínimo los exigidos para la adquisición de software, es decir que incluyan el **plan de cuentas,** el plan de auditoría y el cierre de puertas traseras. Además toda solicitud de modificación al software deberá contar con estudios de factibilidad y de viabilidad al igual que las autorizaciones respectivas de la Universidad.

4.2 Para garantizar la integridad y confidencialidad de la información administrable por el software desarrollado se deberán realizar pruebas intrínsecas al desarrollo y a la documentación técnica respectiva antes del paso a pruebas. Para todo desarrollo de software se deberán emplear herramientas, que permitan tener certeza de que su comportamiento es seguro y confiable. Sólo las funciones descritas y aprobadas en el documento de especificaciones de la solución tecnológica, podrán ser desarrolladas.

4.3 Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción (encriptores).

4.4 Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados. La suficiencia de éste material deberá ser determinada por los usuarios responsables en la entidad.

5. Pruebas del Software.

5.1 Un grupo especializado deberá hacer las pruebas en representación de los usuarios finales. El área de desarrollo de sistemas deberá entregar el software

desarrollado con códigos fuentes al área encargada de ejecutar pruebas, el cual se encargará de la revisión con el fin de detectar códigos malintencionados y debilidades de seguridad utilizando preferiblemente herramientas automáticas, para posteriormente compilarlo e iniciar las respectivas pruebas.

5.2 Con el fin de garantizar la integridad de la información de productos software que se encuentren en etapas de elaboración, deberán ser debidamente planeados, ejecutados, documentados y controlados sus resultados. Además los tipos de pruebas mínimas deberán ser establecidas por la Universidad, teniendo en cuenta que el ambiente de pruebas deberá tener la mayor similitud posible en cuanto a configuración con el ambiente real donde será implantado.

5.3 Las pruebas del software tanto interno como externo deberán contemplar aspectos funcionales, de seguridad y técnicos. En caso de que se requieran las claves para efectuar las pruebas, inserción y mantenimiento del producto, estas se deberán ejecutar de manera segura. La entidad desarrolladora de software deberá establecer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados, el cronograma sólo podrá verse afectado, por eventos de urgencia que sean solicitados por las directivas de la institución.

5.4 El equipo de pruebas deberá garantizar la atención de requerimientos de problemas presentados en el desarrollo de estas. Dicho equipo contará con instrumentos que permitan dejar evidencias del estado de las pruebas.
5.5 Al finalizar los cambios al software, deberá hacerse una serie de pruebas integrales, que garanticen su correcto funcionamiento.

6.Implantación del Software:

6.1 Siempre que se vaya a implementar un software deberá contar con una autorización por escrito de la persona responsable para tal fin. Cualquier característica que no sea necesaria en el ambiente informático de la universidad se identificarán y se desactivarán en el momento de la instalación.

6.2 Siempre que se vaya a implementar un software deberá verificarse que se haya realizado la divulgación y entrega de la documentación, la capacitación y certificación del personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de instalación. La universidad deberá establecer un cronograma de puesta en marcha en producción con el fin de minimizar el impacto del mismo.

6.3 Los módulos ejecutables jamás deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área destinada a tales efectos, que en ningún caso deberá ser el área de desarrollo ni de producción.

6.4 Los programas en el ambiente de producción de la entidad, serán modificados únicamente por personal autorizado y cuando se requiera por fuerza mayor en concordancia con las normas institucionales establecidas.

6.5 Cuando por alguna circunstancia se deban entregar programas desarrollados por la universidad a clientes, compañías comerciales y otros terceros, estos deberán firmar un acuerdo que declare que ellos no desensamblarán, modificarán ni usarán indebidamente tales programas.

7. Mantenimiento del Software

7.1 El área de desarrollo de sistemas no podrá efectuar cambios al software de producción sin las respectivas autorizaciones por escrito y sin cumplir con los procedimientos establecidos por la entidad. La universidad contará con un procedimiento de control de los cambios efectuados que garanticen que sólo se realizan las modificaciones que han sido autorizadas.

7.2 La documentación referente a los cambios hechos al software en la universidad, se preparará simultáneamente con el proceso de cambio. Considerando además que cuando un tercero efectúe modificaciones al software de la universidad, este deberá firmar un acuerdo de no-divulgación y utilización no autorizada del mismo.

7.3 Para cada mantenimiento a la versión del software de misión crítica y prioritaria de la entidad, se actualizará el depositado en custodia en el sitio alterno y el respaldado en la institución. Este software y su documentación se verificarán y certificará su actualización.

7.4 Las actualizaciones de software requerido de la entidad deberán cumplir con los procedimientos de licenciamiento respectivo.

C. DATOS: Respecto a la clasificación, almacenamiento y administración de la información-Datos. Cada funcionario de la universidad es responsable de la información que maneje y deberá seguir los siguientes lineamientos para protegerla, evitar pérdidas, evitar accesos no autorizados y utilización indebida de la misma.

1. Clasificación de la información.

1.1 Todos los datos propiedad de la universidad se deben clasificar dentro de las siguientes categorías para los datos sensibles: SECRETO (ALTO), CONFIDENCIAL(MEDIO), PRIVADO(BAJO); para los datos no sensibles la categoría es PUBLICO (NO APLICA). Para identificar la clase de información y las personas autorizadas para accederla, se deben utilizar prefijos como indicadores generales, tales como: Financiera, Académica, Jurídica, etc. Cualquier información

confidencial y privada debe marcarse (etiquetarse) según las normas de la Universidad. Cualquier dato que se llegue a divulgar por cualquier medio debe mostrar la clasificación de la sensibilidad de la información.

1.2 La universidad debe contar con una metodología que le permita clasificar la información (conforme al numeral 1.1) y conocer su valor. (Pudiera ser el análisis de riesgos).

1.3 Las clasificaciones de sensibilidad de la información deben proteger la información más sensible y se debe clasificar con el máximo nivel de restricción que contenga la misma. De ser necesario compartir información sensible desde estaciones de trabajo, se deben utilizar seguridades ofrecidas por los sistemas para restringir el acceso a través de claves o usuarios específicos.

1.4 La información que se clasifica dentro de las categorías de sensibilidad debe identificarse con la marca correspondiente, indicándose además la fecha en que deja de ser sensible. Lo anterior aplica para información reclasificada tanto a nivel superior como inferior de sensibilidad.

1.5 La responsabilidad en la definición de la clasificación de la información debe ser tanto del dueño de la información como del área encargada de la seguridad informática en la universidad; además se debe contar con una programación para realizar mantenimiento a la clasificación de sensibilidad de la información.

1.6 Cualquier eliminación de información debe seguir procedimientos seguros y debidamente aprobados por el responsable de la seguridad informática y de datos de la entidad.

2. Almacenamiento de la Información

2.1 Almacenamiento Masivo y Respaldo de Información.

2.1.1 Toda información secreta debe ser encriptada, ya sea que se encuentre al interior de la entidad o externamente, en cualquier medio de almacenamiento, transporte o transmisión.

2.1.2 Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un periodo de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada; sin embargo, la información no se debe guardar indefinidamente por lo cual debe determinarse un periodo de tiempo máximo de retención para el caso en que no se haya especificado tiempo.

2.1.3 La información clasificada como sensible (secreta, confidencial o privada) debe tener un respaldo; además, debe tener copias recientes completas en un

sitio externo a la Universidad o en un lugar lejano a donde resida la información origen; en caso de que no se tengan copias de la información crítica, no se deben llevar a cabo procesos de restauración, puesto que se corre el riesgo de perder el original que se tiene.

2.1.4 Todos los medios físicos donde información de valor, sensitiva y crítica sea almacenada por periodos mayores de seis (6) meses, no deben estar sujetos a una rápida degradación o deterioro.

2.1.5 Respecto a los respaldos de información de valor o sensible deben tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite. Los medios magnéticos deben mantenerse almacenados bajo condiciones ambientales de temperatura y humedad óptimas que permitan la conservación de la información.

2.1.6 Toda información contable, de impuestos y de tipo legal debe ser conservada de acuerdo con las normas legales vigentes.

2.1.7 La entidad debe contar con un procedimiento para la restauración de los backups en caso de ser necesario.

2.2 Almacenamiento en forma impresa o documentos en papel

2.2.1 La remisión de información sensible tanto por correo interno como externo debe cumplir con los procedimientos establecidos de manera que se realice en forma segura.

2.2.2 Para todos los mensajes remitidos en formato libre de texto que contengan información sensible para la Universidad debe numerarse cada línea y los documentos oficiales de la universidad que se realicen a mano deben ser escritos con tinta.

2.2.3 La información sensible que aparece en los recibos generados por computador entregados a los solicitantes debe ser truncada.

2.2.4 Todas las copias de documentos secretos deben ser numeradas individualmente con un número secuencial para que las personas responsables puedan localizar rápidamente los documentos e identificar algún faltante de la misma.

2.2.5 Cuando se utilicen medios de transmisión como el fax, se deben seguir los procedimientos establecidos de tal manera que se asegure la confidencialidad e integridad de la información.

3. Administración de la Información

3.1 Respecto a cualquier tipo de información interna de la Universidad, esta no debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al sentido o razón social de la UIS y se debe cumplir con los procedimientos de autorización internos para los casos en que se requiera.

3.2 Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por los empleados de la universidad, durante el tiempo que dure su relación laboral, son de propiedad exclusiva de la entidad.

3.3 Respecto a los datos y programas de la Universidad, estos deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso a oficinas o cuartos de información debe restringirse únicamente a personal autorizado.

3.4 Cuando la información sensible no se está utilizando se debe guardar en los sitios destinados para esto, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.

3.5 En cualquier momento, el propietario de la información con la participación del responsable de la seguridad informática y de datos puede reclasificar el nivel de sensibilidad inicialmente aplicado a la información.

3.6 El acceso a la información secreta se debe otorgar únicamente a personas específicas.

3.7 Toda divulgación de información secreta, confidencial o privada a terceras personas debe estar acompañada por un contrato que describa explícitamente qué información es restringida y cómo puede o no ser usada.

3.8 Toda la información de la Universidad debe contemplar las características de Integridad, Confidencialidad, Disponibilidad, Auditabilidad, Efectividad, Eficiencia, Cumplimiento y Confiabilidad.

3.9 Todo software que comprometa la seguridad del sistema se custodiará y administrará únicamente por personal autorizado. Adicionalmente, se dejará rastros de auditoría de su utilización.

3.10 La realización de copias adicionales de información sensible debe cumplir con los procedimientos de seguridad establecidos para tal fin.

3.11 La información de la universidad no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de la entidad.
3.12 Todos los medios de almacenamiento utilizados en el proceso de construcción, asignación, distribución o encripción de claves o PIN se deben someter a un proceso de eliminación (zeroization) inmediatamente después de ser usados.

3.13 Toda información histórica almacenada debe contar con los medios, procesos y programas capaces de manipularla sin inconvenientes, esto teniendo en cuenta la reestructuración que sufren las aplicaciones y los datos a través del tiempo.

3.14 Las claves y criptogramas para generación y validación de PIN, deben ser manejados en forma dual, es decir, que intervenga más de una persona en el proceso de generación de estas.

3.15 Cuando las palabras claves o números de identificación personal (PIN) sean generados por el sistema, se deben imprimir inmediatamente y nunca se deben almacenar en los sistemas.

4. Validaciones, controles y manejo de errores

4.1 Con el objeto de reducir la probabilidad de ingreso erróneo de datos de alta sensibilidad, todos los procedimientos de ingreso de información deben contener controles de validación.

4.2 Se deben tener procedimientos de control y validaciones para las transacciones rechazadas o pendientes de procesar, además de tiempos determinados para dar la solución y tomar las medidas correctivas.

4.3 Todas las transacciones que ingresen a un sistema de producción computarizado, deben ser sujetos a un chequeo razonable, chequeos de edición y/o validaciones de control.

4.4 Todos los errores cometidos por los empleados de la Universidad y que sean detectados por los clientes deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecidos.

4.5 La Universidad debe utilizar cifras de control, así como definir procedimientos para el cuadre de estas cifras de control, que garanticen la integridad de la información procesada.

4.6 Los controles establecidos en los procesos y las vulnerabilidades de seguridad detectados en los procesos y recursos informáticos de la Universidad, no pueden ser dados a conocer a terceros por parte de los empleados.

D. HARDWARE

La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones debe tomar en cuenta los siguientes criterios para proteger la integridad técnica de la Universidad.

1. Cambios al Hardware

1.1 Los equipos de cómputo de la Universidad no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el aval, evaluación técnica y autorización del área responsable.

1.2 Respecto a daños o pérdidas de equipos propiedad de la entidad que estén al cuidado de empleados de la Universidad, estos deben reportarse a los entes respectivos. La intervención directa para reparar el equipo esta totalmente prohibida. La Universidad debe encargar a personal interno o externo para la solución del inconveniente.

1.3 Todos los equipos de la Universidad deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

1.4 Todo el hardware que adquiera la entidad debe conseguirse a través de canales de compra estándares.

1.5 Para todos los equipos y sistemas de comunicación utilizados en procesos de producción en la Universidad, se debe aplicar un procedimiento formal de control de cambios que garantice que solo se realicen los cambios autorizados. Este procedimiento de control de cambios debe incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado. Así mismo, se debe contemplar la aprobación de la configuración de los parámetros de seguridad y verificar que su instalación no afecta la seguridad establecida en la entidad.

1.6 Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.

1.7 Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.

2. Acceso físico y lógico

2.1 Todas las estaciones de trabajo de la Universidad, antes de ser conectadas a la red interna deben ser autorizadas por el área responsable del hardware.

2.2 Todos los computadores multiusuarios y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.

2.3 Las bibliotecas de cintas magnéticas, discos y documentos se deben ubicar en areas restringidas dentro del centro de cómputo y en sitios alternos con acceso únicamente a personas autorizadas.

2.4 Con la excepción de las computadoras portátiles y los equipos de telecomunicaciones, se debe prohibir el uso de *módems* que establecen conexiones de marcado directo. Todas las conexiones con los sistemas y redes de la entidad deben ser dirigidas a través de dispositivos probados y aprobados por la organización y contar con mecanismos de autenticación de usuario.

2.5 Los equipos de computación de la Universidad que pueden ser accedidos por terceros a través de diversos canales como: líneas conmutadas, redes de valor agregado, Internet y otros, deben ser protegidos por mecanismos de control aprobados por el área de seguridad informática y de datos.

2.6 Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la entidad deben ser restringidas.

2.7 Todas las líneas conmutadas que permitan el acceso a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (*firewall*) antes de que la pantalla de *login* aparezca en la terminal del usuario.

2.8 En el momento de actualizar el inventario de los recursos informáticos de la Universidad se deben tener en cuenta aspectos como: equipos para dar de baja, manejo de partes y repuestos y adquisición de equipos microinformáticos.

3. Respaldo y Continuidad del Negocio

3.1 La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.

3.2 Los microcomputadores y estaciones de trabajo se deben equipar con unidades suplementarias de energía eléctrica (UPS), filtros eléctricos, supresores de picos de corriente y en lo posible, eliminadores de corriente estática.

3.3 Los sistemas de computación y de comunicaciones deben en lo posible estar geográficamente dispersos.

3.4 El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único de conmutación que cause la caída de todos los servicios.

3.5 Los backups de los sistemas de computación y redes deben ser almacenados en una zona diferente de donde reside la información original. Estas zonas de varían de edificio a edificio y son definidas por el área de seguridad de la entidad.

3.6 A todo equipo de cómputo, comunicaciones y demás equipos de soporte debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

3.7 Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

4. Otros

4.1 Todos los procesos relacionados con encripción de datos deben ser soportados preferiblemente por módulos de hardware. Este sistema minimiza la amenaza de ingeniería de reverso del software y una revelación de la(s) clave(s).

4.2 Ningún equipo portátil de computación (*laptop, notebook, palmtop*, etc.) debe registrarse como equipaje de viaje. Estos deben llevarse como equipaje de mano.

4.3 Los equipos portátiles de computación que contengan información sensible deben utilizar software de encripción para proteger la información.

4.4 Todo equipo de cómputo y de comunicaciones de la entidad debe tener un número (lógico y físico) de identificación permanente grabado en el equipo; además, los inventarios físicos se deben realizar en forma periódica, regular y eficiente.

4.5 Todo equipo portátil debe tener la *Declaración de Responsabilidad*, que incluya instrucciones de manejo de información y acato de normas internas y de seguridad para el caso de robo o pérdida.

E. INSTALACIONES FISICAS

Todos los empleados o funcionarios de la Universidad deberán seguir las siguientes pautas de seguridad física con el fin de proteger los recursos técnicos y humanos de la entidad.

1. Control de acceso físico

La Universidad debe contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes y sistema de alarmas, en las dependencias que la misma considere críticas.

1.1 Personas

1.1.1 Los visitantes deben permanecer escoltados y portar un distintivo o escarapela claramente visible, y las personas que laboran para la entidad que requieran ingresar a áreas críticas también deben permanecer escoltadas. Además, tanto los visitantes como los empleados mencionados, únicamente deben tener acceso a la información y recursos necesarios para el desarrollo de sus actividades.

1.1.2 En el caso de que los funcionarios dejen de tener vínculos laborales con la Universidad, todos sus códigos de acceso deben ser cambiados o desactivados. La escarapela, tarjeta de acceso y/o carnet deben ser devueltos a la entidad. En caso de pérdida de la escarapela o tarjeta de acceso también deben desactivarse dichos códigos.

1.1.3 Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.

1.1.4 Como mecanismo de prevención, todos los empleados y visitantes no deben comer, fumar o beber en el centro de cómputo o instalaciones con equipos tecnológicos, al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.

1.1.5 Respecto a las reuniones de trabajo donde se discute y maneja información sensible, se deben realizar en salas cerradas para que personas ajenas a ella no tengan acceso.

1.1.6 Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

1.1.7 Se debe advertir a los funcionarios sobre tener especial cuidado de no permitir el paso al personal no autorizado hacia áreas restringidas cuando los funcionarios autorizados están ingresando a las mismas (piggybacking).

1.2 Equipos y Otros Recursos

1.2.1 Toda sede y equipo informático, ya sean propios o de terceros, que procesen información para la Universidad o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física que se emitan, con el fin de evitar el acceso a personas no autorizadas a las áreas restringidas donde se procese o mantenga información secreta, confidencial y privada, y asegurar la protección de los recursos de la plataforma tecnológica y su información.

1.2.2 Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa del Administrador del Departamento involucrado.

1.2.3 Todos los equipos propiedad de la Universidad como máquinas de escribir, teléfonos celulares, equipos portátiles, módems y equipos relacionados con sistemas de información NO deben retirarse de las instalaciones físicas por ningún personal, a menos que esté previamente autorizado.

1.2.4 Todo maletín, caja o bolso debe ser revisado por personal de seguridad tanto al momento de acceder a las instalaciones como al momento de salir de ellas.

1.2.5 No se debe proveer información sobre la ubicación del centro de cómputo, como mecanismo de seguridad.

2. Protección física de la información

2.1 Todos las personas que laboren para la Universidad y/o aquellas designadas por la Universidad para trabajar en actividades particulares (consultores y contratistas) son responsables del adecuado uso de la información suministrada para tal fin por lo cual se debe velar por su integridad, confidencialidad, disponibilidad y auditabilidad. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

2.2 Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la Universidad. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

2.3 Las áreas donde se maneja información confidencial o crítica deben contar con cámaras que registren las actividades realizadas por los funcionarios.

3. Protección contra desastres

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre (cortos circuitos, vandalismo, fuego, fugas químicas, movimiento de materiales peligrosos, y otras amenazas etc.) puede afectar el nivel de servicio y la imagen de la entidad, se debe prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

4. Planes de emergencia, contingencia y recuperación

4.1 Es responsabilidad de la administración de la Universidad el preparar, actualizar periódicamente y regularmente probar los planes de Contingencias, Emergencias y Recuperación previendo la continuidad de los procesos críticos para el negocio en el evento de presentarse una interrupción o degradación del servicio.

4.2 La Administración debe establecer, mantener y probar periódicamente el sistema de comunicación que permita a los usuarios de la plataforma tecnológica notificar posibles intromisiones a los sistemas de seguridad; estos incluyen posibles infecciones por virus, intromisión de hackers, divulgación de información no autorizada y debilidades del sistema de seguridad.

4.3 El plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre, permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos de negocio, en un tiempo razonable para cada caso y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

4.4 El mantenimiento del plan de Contingencias y Recuperación general debe incluir, entre otros, un proceso estándar que integre los planes de contingencia para computadoras y comunicaciones, así como también el inventario de hardware y software existente y los procesos que correrán manualmente por un periodo de tiempo.

F. ADMINISTRACIÓN DE SEGURIDAD INFORMATICA

En esta sección se establecen las funciones y responsabilidades del área de Seguridad Informática.

1. Generalidades

1.1 Definir, implementar, controlar y mantener las políticas, normas, estándares, procedimientos, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad e integridad de la información de la entidad donde se encuentre (aplicaciones, bases de datos, sistemas operativos, redes, backups y medios).

1.2 Establecer, mantener y administrar una arquitectura de seguridad para la Universidad, además de propiciar y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.

1.3 El departamento o área de Seguridad Informática debe estar ubicado organizacionalmente de manera que tenga autonomía e independencia frente a las demás áreas de tecnología tales como: soporte, diseño y desarrollo, entre otras.

1.4 Representar a la Universidad ante eventos u organizaciones externas sobre temas de seguridad de la información.

1.5 Promover que los planes estratégicos y de operaciones de la Universidad estén en concordancia con las estrategias de seguridad de la entidad educativa.

1.6 Velar porque las excepciones a las políticas de seguridad informática estén autorizadas únicamente por la Dirección o Rectoría de la Organización, de las cuales se debe dejar constancia de los riesgos que en forma consciente se están asumiendo y el periodo de vigencia de la excepción.

2. Funciones de Control

2.1 Establecer e implementar un plan de Seguridad que permita controlar el entorno lógico y físico de la información estratégica de la entidad, teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad y no repudiación de la información.

2.2 Participar activamente en los proyectos informáticos de la Universidad para proveerlos de las seguridades adecuadas, dirigiendo los de Seguridad Informática.

2.3 Especificar las directrices básicas de Seguridad Informática para la definición de los diferentes requerimientos en la adquisición de tecnología (hardware y software) en la Universidad, y vigilar porque se realicen las pruebas de seguridad a los Sistemas de Información.

2.4 Colaborar activamente en el equipo de trabajo de análisis, implementación y mantenimiento de los perfiles de usuario que interactúan con los Sistemas

Operativos, Bases de Datos y Aplicaciones, y cuidar de que en producción únicamente estén los autorizados y vigentes.

2.5 Poseer mecanismos de monitoreo para detectar oportunamente procedimientos inseguros para los Sistemas Operacionales, Aplicativos, Datos y Redes. Usar herramientas adecuadas para la detección de vulnerabilidades en los recursos informáticos, detección de intrusos y test de penetración.

2.6 Investigar métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y realizar reportes periódicos acerca de su efectividad a la Alta Dirección.

2.7 Orientar, recomendar y aconsejar a todos los usuarios de los sistemas de información de la Universidad en cuanto a la seguridad de la información.

2.8 Interactuar tanto en la gestión administrativa como de ejecución a los organismos de control interno y externo.

2.9 Gestionar para que la Universidad cuente con ambientes independientes de Desarrollo, Pruebas, Producción y Capacitación.

2.10 Asegurar que todos los mantenimientos a los sistemas de misión crítica y prioritaria estén autorizados, probados e implementados de acuerdo con los requerimientos de los usuarios previamente validados por un grupo especializado y que no comprometan la seguridad informática de la organización. También, que los sistemas de información queden correctamente documentados y se de la capacitación necesaria a los usuarios finales.

2.11 El Área de Seguridad Informática, es responsable de hacer la revisión continua de las Políticas de Seguridad Informática por lo menos una vez al año.

3. Comité de Seguridad Informática

3.1 Conformar y liderar un Comité de Seguridad Informática, en el cual se sustente el plan de Seguridad Informática a ejecutar en la Universidad desarrollado por el área.

3.2 Dicho comité analizará la administración de problemas de seguridad y definirá las estrategias a implementar que permitan el control del entorno lógico y físico de la información estratégica de la Universidad.

4. Sustentar investigaciones a Investigaciones

4.1 Sustentar las investigaciones sobre violaciones a la seguridad de los sistemas en apoyo al área de Seguridad no Tecnológica (Física) y presentar los informes respectivos a la Dirección de la Organización.

4.2 Investigar, documentar e informar a los propietarios de la información los incidentes de seguridad tanto lógica como física.

4.3 Efectuar un seguimiento a las acciones disciplinarias y legales asociadas con los incidentes de seguridad investigados.

5. Elaboración del Mapa de Riesgo

Realizar estudios de análisis de riesgos en Seguridad Informática con el fin de identificar oportunamente los eventos o situaciones que atenten contra la integridad, confidencialidad, auditabilidad y disponibilidad de la información presentados en la Universidad, definiendo planes de acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.

6. Plan de Contingencia

6.1 Participar, implementar y mantener el Plan de Emergencia, Contingencia y de Recuperación de desastres y continuidad del negocio relacionados con tecnología informática.

6.2 Verificar el proceso de pruebas que se debe ejecutar periódicamente a los Planes de Emergencia, Contingencia y de Recuperación.

7. Capacitación y Entrenamiento

7.1 Determinar y apoyar a las áreas encargadas en la ejecución de un plan de capacitación continuo que permita actualizar a los funcionarios en aspectos de seguridad informática fortaleciendo la cultura sobre el tema.

7.2 Dar un entrenamiento adecuado a los usuarios, custodios, y usuarios dueños de la información en cuanto a los requerimientos y responsabilidades sobre la seguridad de la información.

G. SEGURIDAD EN REDES DE COMUNICACIÓN
(Ambiente y Servicios)

1. Ambiente

Los funcionarios de los distintos campus de la Universidad responsabilizados de las redes de comunicación deberán seguir los siguientes disposiciones para proteger la información que por ellas fluya:

1.1 Aspectos Generales

1.1.1 Toda información secreta y/o confidencial que viaje por las redes de comunicación de la Universidad deberá estar encriptada.

1.1.2 La Universidad deberá propiciar el establecimiento de un mecanismo de administración e intercambio robusto de Llaves Lógicas para los procesos de encripción como por ejemplo, plataformas de llaves públicas (PKI).

1.1.3 Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la Universidad deberán ser tratadas como información confidencial.

1.1.4 Los empleados y contratistas no deben llevar a cabo ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, módems, ni cambiar su configuración sin haber sido formalmente aprobados por el área responsable en la Universidad.

1.1.5 Las centrales de conexión o centros de cableado deben ser catalogados como zona de alto riesgo, estos sitios se consideran zona roja con limitación y control de acceso.

1.1.6 Los empleados o contratistas no deben llevar a cabo ningún tipo de instalación a los canales de transmisión de datos, deben instalarse con una previa autorización formal de las áreas responsables de la Universidad.

1.2 Conexiones con redes públicas e Internet.

1.2.1 Toda conexión entre las redes de la Universidad y redes externas de servicios (Outsourcing), redes públicas e Internet deberán contar como mínimo con mecanismos de control de acceso lógico, tales como, Firewall, proxys, Dns, entre otros; igualmente todos los usuarios deberán autenticarse ante estos mecanismos de seguridad; en caso de no contar con estos, la conexión a Internet deberá establecerse en un equipo independiente a la red de comunicaciones de la Universidad.

1.2.2 Esta prohibido toda conexión a través de módems (dial-up) a estaciones de trabajo que estén simultáneamente conectadas a una red de área local o a otra red de comunicación interna.

1.3 Conexiones a redes amplias, redes metropolitanas y locales.

1.3.1 La red de amplia cobertura geográfica con cobertura nacional e internacional o la red metropolitana deberán estar divididas en forma lógica y contar con mecanismos de control perimetral y de control de acceso.

1.3.2 La Universidad deberá inclinarse por segmentar las redes de comunicaciones de tal forma que los usuarios conserven independencia sobre las mismas.

1.3.3 Es aconsejable la utilización de la facilidad "call-back" para garantizar que el acceso remoto se hace a personal autorizado y registrado para utilizarlo.

2. Servicios

2.1 Aspectos Generales.

2.1.1 Lo publicado en las páginas World Wide Web (www) debe ser autorizado por el área competente de la Universidad. Los empleados que se enteren de la existencia de publicados de páginas no autorizadas, deben informar inmediatamente al área responsable.

2.1.2 El contenido de las páginas Web debe estar de acuerdo con las políticas de la Universidad, debe tener medidas de seguridad y se debe ajustar a los estándares de diseño, navegación y redacción establecidos.

2.1.3 Si se crea un buzón en el Web de la Universidad para recibir comentarios y sugerencias, este debe contener textos que indiquen que la recepción de ideas no solicitadas por la Universidad no obliga a la misma a mantener confidencialidad sobre estas, ni a pagar derechos de autor.

2.1.4 Con excepción del correo electrónico, todos los accesos a Internet, deben ser aprobados previamente por el área responsable.

2.1.5 La información confidencial correspondiente a los accesos de los sistemas de comunicación e información de la universidad, como números telefónicos de marcación de módems, no debe ser expuesta en boletines electrónicos ni en directorios telefónicos.

2.1.6 El uso de los sistemas de la Universidad para entrega o intercambio electrónico de datos con terceros, se puede hacer sólo si existe un contrato que establezca los términos y condiciones de estos procesos. Este contrato debe ser aprobado por la alta gerencia o por el área responsable.

2.1.7 Los accesos a Internet/Intranet para utilizar sistemas de información de la Universidad, en forma remota y en tiempo real deben ser autorizados por el área de seguridad informática.

2.1.8 Los computadores y las herramientas de comunicación de la Universidad tales como: correo de voz, boletines electrónicos, sistemas administrativos de bases de datos, facilidades de correo electrónico, entre otros, no deben ser usados para discutir o comentar cambios o políticas organizacionales sin la previa autorización de la Universidad.

2.1.9 Los empleados no deben establecer carteleras electrónicas de anuncios, redes locales, conexiones vía módem a la red interna de la entidad, sin la previa autorización del área de seguridad informática.

2.1.10 La Universidad debe generar normas en donde se establezcan los aspectos de seguridad que se deben contemplar al compartir recursos informáticos.

2.2 Internet

2.2.1 Las leyes para derechos de reproducción, patentes, marcas registradas y todo lo relacionado con derechos de autor aplican en Internet.

2.2.2 Todo mensaje publicado por los empleados en un grupo de discusión de Internet, en un boletín electrónico, o en cualquier otro sistema de información público, debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la Universidad. Únicamente pueden indicar su afiliación aquellas personas autorizadas explícitamente por la alta dirección.

2.2.3 Todos los directorios públicos con permiso de escritura que se encuentren en computadores de la Universidad y estén conectados a Internet, deben ser revisados y borrados periódicamente, para evitar saturación de máquinas e intercambio de información ilegal.

2.2.4 Todo el software obtenido a través de Internet debe ser revisado por un software antivirus (filtros de contenido), antes de transmitirlo internamente hacia usuarios de la organización.

2.2.5 El uso de sistemas de cómputo de la Universidad para tener acceso a Internet con fines personales no es permitido. Todos los empleados deben estar enterados que existe un log de auditoría que refleja las transacciones realizadas en este medio, así como las implicaciones legales por la instalación de software no registrado en la Universidad.

2.2.6 Los empleados que accidentalmente se conecten a páginas de Internet que tengan contenidos sexuales, racistas o cualquier otro tipo de material ofensivo

deben desconectarse inmediatamente e informar a su superior, para que sean bloqueados estos accesos.

2.2.7 La entidad debe establecer normas para proteger la confidencialidad y privacidad de la información (disclaimers) obtenida a través de sus servicios de Internet teniendo en cuenta los siguientes parámetros: tipo de información que se muestra (transaccional o informativa), condiciones de uso y acceso, garantías ofrecidas (por la información y por los medios de comunicación), límite de responsabilidad por perjuicios que pueda ocasionar la información contenida en la página y derecho de propiedad.

2.3 Intranet

2.3.1 La información que se publique en la Intranet de la Universidad, debe contar con la aprobación del responsable del área encargada de la página y la del propietario de la información involucrada.

2.3.2 El material que se publique en la Intranet de la Universidad debe ser revisado previamente para confirmar la actualidad, oportunidad e importancia de la información y evitar que los programas incluyan virus y/o caballos de Troya. Así mismo, se debe evaluar posibles problemas operativos y de seguridad de acuerdo a las políticas establecidas por el área de seguridad informática.

2.3.3 La información de Intranet debe ser únicamente utilizada por personal autorizado. Los empleados no deben redireccionar información que aparezca en Intranet a terceros sin autorización de la entidad.

2.3.4 La Universidad debe generar procedimientos para la administración y manejo de la información en la Intranet, en especial el mantenimiento y depuración de la información publicada.

2.4 Correo Electrónico

2.4.1 El envío de mensajes masivos a través de correo electrónico y correo de voz debe ser realizado solo con aprobación de la alta dirección.

2.4.2 El correo electrónico no debe ser utilizado por terceros (clientes o proveedores) sin previa autorización.

2.4.3 La información confidencial no debe ser transmitida por correo electrónico, a menos que lo autorice la alta dirección, en cuyo caso los archivos deben viajar en forma encriptada.

2.4.4 Los empleados no deben utilizar una cuenta de correo electrónico que pertenezca a otro trabajador, si hay necesidad de hacerlo en caso de ausencias o

vacaciones se debe recurrir a mecanismos alternos como redirección de mensajes.

2.4.5 Los empleados no deben enviar mensajes de correo electrónico con contenidos hostiles que molesten a los receptores del mismo, como comentarios sobre sexo, raza, religión o preferencias sexuales, así mismo cuando un empleado reciba este tipo de mensajes debe comunicarlo a su jefe inmediato y al área encargada de personal.

2.4.6 Ningún empleado esta autorizado para monitorear los mensajes de correo electrónico, excepto las áreas de control o áreas responsables. El monitoreo es realizado para cumplir con políticas internas en casos de sospechas de actividad no autorizada, investigaciones y otras razones de la alta dirección, la Universidad no esta obligada a solicitar autorización del empleado involucrado.

2.4.7 El sistema de correo electrónico de la Universidad debe ser usado únicamente para propósitos de trabajo. Todos los mensajes enviados por este medio pertenecen a la Universidad y ésta se reserva el derecho de accesar y revelar los mensajes enviados por este medio para cualquier propósito.

2.4.8 Los empleados no deben utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica ha sido firmada por la persona que la envía.

2.4.9 La Universidad debe establecer normas para proteger la confidencialidad y privacidad de la información (disclaimers) obtenida a través de sus servicios de correo electrónico, teniendo en cuenta los siguientes parámetros: tipo de información que se obtiene, finalidad que se dará a la información, modificación o actualización de la información, aceptación de los términos por las partes involucradas.

2.4.10 La Universidad debe establecer procedimientos para el manejo de carpetas públicas, archivos adjuntos enviados en los mensajes, archivo de la información enviada/recibida y utilización de firma digital y codificada.

2.5 Outsourcing

2.5.1 La conexión entre sistemas internos de la entidad y otros sistemas (de terceros) debe ser aprobada y certificada por el área de seguridad informática con el fin de no comprometer la seguridad de la información interna de la entidad.

2.5.2 La Universidad debe llevar a cabo inspecciones sorpresivas a los sistemas de comunicación de terceros para velar porque la información se esté manejando con las normas de seguridad acordadas.

H. SEGURIDAD EN SISTEMAS DE INFORMACIÓN Y SISTEMAS OPERATIVOS

Controles de Seguridad para cualquier Sistema de Información y Sistema Operativo

Todos los Sistemas de Información y Sistemas Operativos de la Universidad deben considerar los aspectos mencionados a continuación y los funcionarios deben velar por su cumplimiento:

1. Controles de Acceso

1.1 Generales

1.1.1 Todos los sistemas automatizados deben utilizar estándares para los códigos de identificación de usuario, para nombres programas y archivos tanto en ambientes de producción como en desarrollo, para nombres de sistemas de información y otras convenciones utilizadas en tecnología.

1.1.2 Cuando el sistema de control de acceso a un computador o red no funciona apropiadamente, debe suspenderse el acceso a todos los usuarios.

1.1.3. Toda transacción que afecte información de valor, sensible o crítica debe ser procesada únicamente cuando se valide la autenticidad del origen (usuario o sistema) y se compruebe su autorización mediante un mecanismo de control de acceso o perfiles.

1.1.4 Todo programa y archivo que contenga fórmulas, algoritmos u otras especificaciones que se utilicen para la generación de claves debe estar controlado con las más altas medidas de seguridad.

1.1.5 Las palabras claves siempre deben estar encriptadas y no se deben incorporar dentro de los programas de software. Los computadores y sistemas de comunicación deben tener implementados controles que impidan la recuperación de palabras claves almacenadas.

1.1.6 Ningún empleado debe construir o utilizar mecanismos para coleccionar passwords o códigos de identificación de usuarios; ni tampoco mecanismos para identificar o autenticar la identidad de los usuarios sin la autorización del Área de Seguridad Informática.

1.1.7 Todas la palabras daves inicialmente emitidas deben ser validas solamente para la primera conexión del usuario, momento en el cual deben ser cambiadas.

1.1.8 El acceso a información secreta únicamente se debe otorgar a personas específicas.

1.1.9 Los códigos de usuario y claves son personales e intransferibles.

1.1.10 La Universidad debe restringir la utilización de usuarios genéricos. Así mismo, debe realizar el control de usuarios, administradores, superusuarios, de emergencia, anónimos, invitados, proveedores y temporales.

1.2 Perfiles y privilegios

1.2.1 Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los funcionarios que acceden el sistema, de tal forma que la información solo sea modificada por los usuarios autorizados y en los horarios establecidos.

1.2.2 Las modificaciones a los privilegios o perfiles de usuario deben ser realizadas por los usuarios administradores a través de pantallazos predefinidos para este fin, previa autorización del dueño de la aplicación o del dueño de la información.

1.2.3 La Universidad debe incluir normas para la administración de usuarios y perfiles en donde se debe dejar evidencia de los cambios realizados a los perfiles, el estado y eliminación de las cuentas.

1.2.4 Los privilegios especiales del sistema deben otorgarse únicamente a los funcionarios administradores del sistema o responsables de la seguridad. Los usuarios finales no deben tener acceso a los niveles de comandos para el funcionamiento del sistema.

1.2.5 Los administradores de los sistemas o superusuarios deben tener por lo menos dos usuarios-Ids: uno de acceso privilegiado y el otro debe ser un usuario-ID ordinario con el que se lleve a cabo el trabajo diario de un usuario común.

1.2.6 El nivel de superusuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

1.2.7 Todas las herramientas de los sistemas de información, construidas o distribuidas por la Universidad, que puedan usarse para causar un daño significativo deben ser automáticamente restringidas para que sean solamente usadas en el(los) propósito(s) determinado(s).

1.2.8 El hardware y software de diagnóstico y/o utilitarios sólo deberán ser usados por personal autorizado y su uso debe ser controlado por el área de seguridad informática en la Universidad.

1.3 Controles automáticos y de usuario.

1.3.1 El control de acceso a todos los sistemas de computación de la Universidad debe realizarse por medio de códigos de identificación y palabras claves únicos para cada usuario.

1.3.2 Si el usuario digita un login (user id o clave) incorrecto, el sistema no debe mostrar la fuente del problema, simplemente debe informársele que el login es incorrecto y terminar la sesión o esperar un nuevo login.

1.3.3 Después de tres intentos consecutivos infructuosos al sistema, se debe suspender el acceso del usuario hasta que el administrador del sistema o responsable de la seguridad lo habilite de nuevo siguiendo con los procedimientos establecidos para identificación del usuario.

1.3.4 Las palabras clave deben tener la siguiente estructura: Longitud mínima de 8 caracteres, de los cuales al menos un carácter alfabético en minúscula, otro en mayúscula y un carácter no alfabético.

1.3.5 Los usuarios deben definir palabras claves que sean difíciles de adivinar, no pueden ser series de números (123456), ni repeticiones de caracteres (AAAA,1111), ni situaciones familiares (fechas de cumpleaños, nombres familiares, placas del carro, etc.), ni palabras compuestas combinadas con cierto número de caracteres que cambian predeciblemente (un área, una fecha, una ciudad, un proyecto, etc.), ni palabras muy similares a otras definidas anteriormente.

1.3.6 El sistema debe llevar un histórico de palabras clave, de tal forma que los usuarios no usen palabras claves utilizadas anteriormente.

1.3.7 La identificación del usuario se debe asignar en forma secuencial y numérica de tal forma que no exista una relación obvia entre la identificación y el nombre verdadero del usuario.

1.3.8 Las palabras claves no se deben presentar en pantalla o impresas.

1.3.9 El sistema debe obligar automáticamente a que todos los usuarios cambien sus palabras claves al menos una vez cada treinta (30) días.

1.3.10 En el momento del login, se le debe dar a cada usuario la información indicando la última hora y fecha del último login. Esto permitirá detectar fácilmente el uso no autorizado del sistema.

1.3.11 A menos que se tenga un permiso especial concedido por el administrador del sistema, el sistema no debe permitir que ningún usuario maneje simultáneamente sesiones múltiples cuando esté en línea.

1.3.12 El sistema debe controlar el tiempo de inactividad del usuario y desactivar la sesión automáticamente.

1.3.13 Los usuarios no deben abandonar su microcomputador, estación de trabajo o terminal sin haber realizado logout o haber cerrado la sesión.

1.3.14 A todos los usuarios se les debe revocar los privilegios automáticamente cuando no han tenido actividad durante un periodo determinado.

1.3.15 Si se utilizan palabras claves generadas por el sistema, éstas se deben generar teniendo como base el tiempo del reloj o alguna otra parte del sistema de procedencia impredecible que cambie frecuentemente.

2. Logs

2.1 Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Universidad, como sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones, deben generar logs de auditoría.

2.2 Todos los archivos de logs deben proporcionar suficiente información para apoyar el monitoreo, control y auditorías. La Universidad se reserva el derecho de revisión de los mismos.

2.3 Todo archivo de log deben incluir como mínimo la siguiente información: (1)identificación del código del usuario, (2) identificación de la terminal, (3), fecha/hora de la entrada y de la salida de cada sesión del sistema, (4) aplicaciones invocadas, (5) cambios de información en los archivos de las aplicaciones críticas (6) adiciones y/o cambios a los privilegios de los usuarios, (7) controles del sistema modificados, (8) fecha/hora de iniciación y terminación de ingreso al sistema de información, (9) Intentos de accesos no autorizados, (10) intentos de uso de privilegios de comandos no autorizados, (11) uso de comandos privilegiados y de software utilitario del sistema.

2.4 Todos los archivos de logs de los diferentes sistemas deben retenerse por periodos definidos según su criticidad y la exigida de ley en forma obligatoria. Además, deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

2.5 Los logs son evidencia digital suficiente de la utilización de los aplicativos, sistemas operacionales y comunicaciones y pueden ser utilizados por la organización en todos los casos que se consideren necesarios (investigaciones

internas, investigaciones externas, consultas de entes externos y de entes de control).

2.6 Las aplicaciones de misión crítica requieren tener archivos de logs robustos que permitan reanudar las actividades del sistema en un tiempo prudente cuando se presente una contingencia.

2.7 Todos los logs habilitados en el sistema deben tener definido un usuario para su administración y control, quien además deberá encargarse de realizar seguimientos y revisiones periódicas a los mismos.

2.8 Todos los computadores de la Universidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en el log sea correcto.

2.9 Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques capaces de detectar y grabar eventos significativos en aspectos de seguridad automática. Estos ataques incluyen intentos de desactivar, modificar, intentar o detectar las claves de acceso al software y/o a los mismos logs.

2.10 Cada vez que se hacen copias adicionales de información sensible, se debe llevar un registro en un log donde se indique el número de copias y cantidad de receptores de éstas.

3. Otros Controles

3.1 Todo sistema debe contener herramientas que ayuden al administrador del sistema en la verificación del estado de seguridad de los sistemas. Estas herramientas deben contener mecanismos que sirvan para detectar, informar y corregir problemas de seguridad.

3.2 Todo software residente en microcomputadores o estaciones de trabajo debe estar protegido contra escritura, de tal forma que se generará una señal de alerta o un error cuando un virus intente modificar o modifique el software.

3.3 Todos los sistemas de información en producción deben ser periódicamente revisados por el área de seguridad informática, para determinar el cumplimiento de un conjunto mínimo de controles requeridos para reducir el riesgo a un nivel aceptable.

3.4 Los discos y otros medios de almacenamiento en línea usados en sistemas en producción no deberán contener compiladores, ensambladores, editores de texto, procesadores de palabra u otras utilidades de propósito general que puedan utilizarse para comprometer la seguridad del sistema.

3.5 Las características que son innecesarias en el ambiente informático de la Universidad se deberán desactivar en el momento de la instalación del software.

3.5 DEFINICIÓN DE PROCEDIMIENTOS ACORDES A POLÍTICAS Y ESTÁNDARES FORMALES DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

Para la definición de los procedimientos de seguridad de la Universidad Industrial de Santander vamos a proponer la siguiente plantilla:

- PLANTILLA ESTÁNDAR DE PROCESOS DE SEGURIDAD: Elementos recomendados de un Procedimiento .

A continuación se muestra el esquema o plantilla de un procedimiento:

NOMBRE DEL PROCEDIMIENTO:
Propósito del procedimiento: o Qué estándar cumple: en este punto se van a encontrar una serie de letras y números que se referirán tanto a la política como al estándar basados en la figura 28, donde se expone el modelo de seguridad informática propuesto, en el que se observan los diferentes componentes diferenciados cada uno por una letra y donde más adelante se exponen cada uno de los estándares. Es decir si en este punto se encuentra la siguiente nomenclatura: **D-3-3.1** representará lo siguiente: **D:** pertenece a la política de Hardware que dice: "La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones debe tomar en cuenta los siguientes criterios para proteger la integridad técnica de la Universidad." **3:** Al estándar representado por este número que dice "Respaldo y Continuidad del Negocio. **3.1:** Se refiere exactamente al número del estándar que cumple el procedimiento el cual dice: "La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros". o Cuál es el objetivo del procedimiento
Alcance del procedimiento: o A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento o Qué función se espera que este proceso ejecute o Los conocimientos previos que se necesitan tener para ejecutar el proceso

Definición del proceso o Introducción al proceso ▪ Descripción de lo qué el proceso hace o Descripción detallada de: ▪ Cómo se ejecutará el proceso ▪ Cuándo se ejecutará el proceso ▪ Lo que se espera que suceda durante la ejecución del proceso ▪ Lo que no se espera que suceda ▪ Las acciones que se tomarán si ocurre un hecho imprevisto ▪ Qué criterios indican la ejecución exitosa del proceso ▪ Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará ▪ Las interacciones requeridas o esperadas de otros procesos	
Problemas de los procesos o Qué se hará si se presenta un problema en el proceso ▪ Error de proceso	
Excepción del proceso por no aplicabilidad	**Responsable**

A continuación (Ver Anexo A) se pretende mostrar y proponer una orientación inicial acerca de cómo se pueden llegar a establecer los procedimientos acordes con el estándar y por supuesto la política, en tal forma que permitan armar un bloque de protección adecuada de seguridad informática para la UIS. Esta muestra inicial de procedimientos se va a describir con base en las amenazas encontradas y descritas en el capítulo 2, siguiendo la plantilla expuesta anteriormente, no sin antes advertir, que debe continuar su revisión y desarrollo con el personal que los vaya a ejecutar, por lo tanto, van a estar sujetos a cambios y mejoras permanentes, con el objetivo de cumplir tanto con el estándar como con la política, permitiendo fortalecer el modelo de seguridad.

Por consiguiente los Coordinadores Funcionales de acuerdo a su experiencia y desarrollando la plantilla propuesta, complementarán, fortalecerán y especializarán cada vez más los procedimientos de seguridad a seguir para que con el análisis y aprobación del Consejo de Seguridad puedan obtener el respaldo de las directivas de la UIS y poder así implantar dichos mecanismos.

3.6 PRESUPUESTO MODELO DE SEGURIDAD INFORMATICA

	AÑO 1	AÑO 2	AÑO 3
INGRESOS	**$ 354.900.000**	**$ 332.400.000**	**$ 332.400.000**
Ingreso UIS-Partida para poner en funcionamiento el consejo de seguridad	$ 354.900.000	$ 332.400.000	$ 332.400.000
EGRESOS	**$ 354.900.000**	**$ 332.400.000**	**$ 332.400.000**
INVERSIONES FIJAS	$ 8.000.000		
Software	$ 1.000.000		
Hardware	$ 9.000.000		
OTRAS INVERSIONES	$ 4.500.000		
GASTOS DE ADMINISTRACIÓN			
Empleados Administrativos del Consejo de Seguridad:	**$ 102.000.000**	**$ 102.000.000**	**$ 102.000.000**
Director de Seguridad Informática			
Experto en legislación informática			
Administrador Central de Seguridad Informática			
Administrador de Usuarios y Accesos			
Director Funcional			
Secretaria			
GASTOS DE OPERACIÓN			
Empleados operativos del Consejo de Seguridad	**$ 230.400.000**	**$ 230.400.000**	**$ 230.400.000**
Coordinador Funcional de Seguridad Informática (4 en la sede principal y 2 en cada uno de los 6 Campus)			
Saldo periodo	$ -		$ -
Saldo anterior	$ -	$ -	$ -
Saldo final	$ -	$ -	$ -

Cuadro 17. Flujo de caja mensual -1 AÑO

	unidades	Unitario	MONTAJE	MES1	MES2	MES3	MES4	MES5	MES6	MES7	MES8	MES9	MES10	MES11	MES12
INGRESOS			$ 22.500.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000	$ 27.700.000
Ingreso UIS-Partida para poner en funcionamiento el consejo de seguridad															
EGRESOS			***$ 22.500.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***	***$ 27.700.000***
INVERSIONES FIJAS															
computadores	**2**	**$2.250.000**	**$ 4.500.000**												
muebles y enseres	**GL**	**$ 1.000.000**	**$ 1.000.000**												
Libros -Manuales etc	**GL**		**$ 2.000.000**												
papelería	**GL**		**$ 500.000**												
Software															
Nmap(Exploración de puertos)	**Free**		**$ -**												
SAINT (Herramienta automática de rastreo)	**Free**		**$ -**												
PGP(Incluye firma digital-encriptamiento de dominio público)	**Free**		**$ -**												
SNORT(paquete de dominio público)	**Free**		**$ -**												
Paswwd+(paquete de dominio público)	**Free**		**$ -**												
SSH (cifrado en la transmisión)	**Free**		**$ -**												
Antivirus(la UIS ya los posee con licencia)	**Free**		**$ -**												
Tripwire(Informa modificaciones archivos)	**1**		**$ 1.000.000**												
Hardware															
Kit de los Coordinadores Funcionales(herramientas para redes)	**10**	**$ 900.000**	**$ 9.000.000**												
OTRAS INVERSIONES															
gastos de organización y legales			**$ 2.000.000**												
Instalación, pruebas y puesta en marcha			**$ 2.000.000**												
Otros (convocatoria proveedores)			**$ 500.000**												
GASTOS DE ADMINISTRACIÓN															
Empleados Administrativos del Consejo de Seguridad:															
Director de Seguridad Informática	**1**	**$ 2.500.000**		**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**	**$ 2.500.000**
Experto en legislación informática	**1**	**$ 1.800.000**		**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**
Administrador Central de Seguridad Informática	**1**	**$ 1.800.000**		**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**
Administrador de Usuarios y Accesos	**1**	**$ 1.800.000**		**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**	**$ 1.800.000**
Director Funcional: Este cargo puede ser desempeñado por los respectivos Coordinadores de las Escuelas, que ahora velarán por la seguridad informática de sus respectivas escuelas(27 Escuelas y 4 en los campus, por lo tanto no influ irán en este gasto de administración)	**31**	**$ 1.800.000**		**$ -**											
Secretaria	**1**	**$ 600.000**		**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**	**$ 600.000**
GASTOS DE OPERACIÓN															
Empleados operativos del Consejo de Seguridad															
Coordinador Funcional de Seguridad Informática(4 en la sedeprincipaly 2 en cada uno de los 6 Campus)	**16**	**$ 1.200.000**		**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**	**$ 19.200.000**
Saldo periodo				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Saldo anterior				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Saldo final				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

4. CONCLUSIONES

- Es necesario hoy en día para cualquier organización ya sea de índole privada o pública trabajar en la seguridad a su información, pero no de una forma parcial o aislada, sino muy por el contrario en forma conjunta, de tal forma que se traduzca en la concepción, diseño y posterior implantación de un modelo de seguridad que respalde los objetivos del negocio.

- La prospectiva puede ser utilizada como una metodología adecuada para efectuar el proceso de análisis de riesgos informáticos.

- La infraestructura de comunicaciones de la UIS, es cada vez más creciente y compleja, provocando paralelamente el aumento de riesgo informático, por lo tanto se observa la necesidad de reforzar controles en la transmisión, envío y recepción de la información mediante servicios de seguridad como: encripción, firma digital, certificado digital y notarías electrónicas, productos que pueden ser desarrollados como proyectos de maestría y de pregrado, brindándole continuidad a este proyecto de investigación.

- Las políticas, estándares y procedimientos de seguridad deben ser respaldados por las directivas de la organización, de lo contrario no se podría consolidar ningún modelo de seguridad informática.

- Los procedimientos de seguridad deben ser establecidos por el personal especializado y directamente encargado de la prevención o corrección de la amenaza informática.

- La red de datos de la universidad debe preocuparse por extender en ciertas áreas críticas el servicio de encriptamiento, pudiera ser con SSH, para proteger la información en tránsito.

5. RECOMENDACIONES

- La UIS debe fomentar una cultura de seguridad informática entre sus empleados, sino se trabaja en este aspecto, cualquier modelo a implantar resultaría inútil. La Web sería un medio bastante importante para concientizar al personal acerca de lo vital que es para la universidad el tema de la seguridad a su información.

- La universidad debe preocuparse por implantar materias, cursos y diplomados afines a la seguridad informática como criptografía, seguridad en Unix, montaje seguro de servidores Web, análisis de riesgos informáticos entre otras, dentro de los planes de estudio de carreras afines a la informática, electrónica y telecomunicaciones.

- El sistema de cámaras de vigilancia debería ser extendido a todas las demás zonas críticas de la UIS, como por ejemplo el lugar donde se encuentra el firewall. Además se debería contar con personal permanente que vigile al instante lo que sucede ante las cámaras y que cuente con comunicación directa con los vigilantes de la universidad, permitiendo tomar medidas preventivas y no correctivas como sucede actualmente, en la que sólo se graban los sucesos para posteriormente guardarlos en cintas de grabación.

- Sería conveniente unificar criterios en la utilización de un único sistema operativo, esto con el ánimo de unificar esfuerzos, acciones y herramientas de seguridad informática comunes tendientes a enfocar los esfuerzos hacia una sola dirección.

- Para mejorar la seguridad de los servidores de Correo, Web y DNS es aconsejable centralizar el montaje y configuración por un comité especializado de la universidad, para que lo haga con las mejores medidas de seguridad, evitando con esto que personal practicante lo efectúe sin la menores normas de seguridad.

- La universidad tiene una fortaleza matemática reconocida y clave para las ingenierías, por lo tanto estas bases pueden permitirle a ingenieros de sistemas como también a matemáticos continuar esta investigación hacia la búsqueda de productos como por ejemplo la firma digital.
- Las medidas de seguridad físicas que tiene el sitio donde está alojado el firewall de la Universidad deben ser reforzadas.
- Las organizaciones actuales sienten necesidad de profesionales especializados en seguridad informática, situación que abre la oportunidad para que la universidad se motive y gestione cursos, diplomado o especializaciones en esta área.

BIBLIOGRAFÍA

CANO, J. (2002) Estado de la Seguridad Informática en Colombia, Revista SISTEMAS, Asociación Colombiana de Ingenieros de Sistemas – ACIS. No.82. Julio-Septiembre.

SHELDON, Tom. Manual de Seguridad de Windows NT, 1 ed. Madrid: McGrawHill, 1997. pp 20-21.

CLARK, David Leon. Guía para el Administrador de Redes Virtuales. 1 ed. México,D.F: McGrawHill, 2000. p. 80-83.

PARSONS, J.J.Conceptos de Computación, 2 ed. México, D.F: Internacional Thomson Editores, 1999.p. G-6.

GUILLEN, Anellie, Boletín No.19. www.gcpglobal.com.

GONZALEZ, G y .MAS, J. El libro de los Virus y la Seguridad Informática, 1 ed. Madrid : Ra-ma, 1990. p. 41-42.

CHAPMAN, D.B. y ZWICKY, E.D. Construya Firewalls para Internet, 1ed. México, D.F: McGrawHill, 1997. p.7-10.

FARLEY,M., y STEARNS, T. Guía de Seguridad e Integridad de Datos, 1 ed. Madrid: McGrawHill, 1998.p.213.

AMOROSO, E.G. Fundamentals of Computer Security Technology ,Prentice Hall, 1994. p.1-4.

KISKENDALL,K.R y LIÚ, D. Fundamentos de Seguridad de Redes-Academia Networking de CISCO System-Especialista en Firewall CISCO, Madrid : Pearson, 2005.p. 832.

RANADE,J. Computer & Comunications Security Strategies for the 1990s , Singapur: McGrawHill,1989.p.1-3.
CROTHERS, T. Network Security and Firewalls: Academic Student Guide, USA: Certified Internet Webmaster.p. 951.

GARFINKEL, S and SPAFFORD, G. Web Security & Commerce, 1 ed. USA: O`Reilly, 2002. p.11.

CHESWICK,W,R and BELLOVIN, S,M. Firewalls and Internet Security. 1 ed. USA: Addinson Wesley, 1994.p.13.

FORD, W. Computer Communicatios Security. 1 ed. USA: Prentice Hall, p.14.

FISHER, R.P. Seguridad en los Sistemas Informáticos.1 ed.: Díaz de Santos, 1988, p.1-3.

SCAMBRAY,J., MCCLURE, S. and KURTZ, G. Hackers 2 – Secretos y soluciones para la seguridad de redes. 1 ed. México: McGrawHill, 2001. p.115, 171, 626-629.

GUERRERO, C.D y VELAZQUEZ, G.A. IX Semana Técnica Internacional: Seguridad Informática. 1 ed. Bucaramanga: Armonía Impresores, 2002, p.

NORTHCUTT, S y NOVAK, J. Detección de Intrusos. 2 ed. Madrid: Prentice may, 2001. 445 p.

SEDISI (Asociación Española de Empresas de Tecnologías de la Información). Guía de Seguridad informática. Madrid, URL: http://www.sedisi.es/05_Estudios/guia04.htm. p. 4-8.

ANEXO A

MANUAL DE PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD INDUSTRIAL DE SANTANDER UIS

NOMBRE DEL PROCEDIMIENTO: Elección Unidades de Potencia Ininterrumpida (UPS) **Observaciones: Evita - amenaza1.** Fluctuaciones en la tensión o frecuencia en el suministro de energía eléctrica
Tipo Procedimiento (P: Preventivo, C: Correctivo): P
Propósito del procedimiento: • **Qué estándar cumple:** D-3-3.1, D-3-3.2, D-3-3.6 • **Cuál es el objetivo del procedimiento:** Evitar indisponibilidad de la información, pérdida de información o daños hardware a equipos.
Alcance del procedimiento: • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a equipos de las salas de cómputo de la D.S.I y en general a toda la red de la UIS y demás campus. • **Qué función se espera que este proceso ejecute**: Proteger contra pérdida inesperada de información y daños de equipos. **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en electricidad (UPS) y equipos de protección computacional.

Definición del proceso

- **Introducción al proceso**

▪ **Descripción de lo qué el proceso hace**: Proteger los equipos y su respectiva información ante eventuales fallos en el fluido eléctrico.

- **Descripción detallada de:**

▪ **Cómo se ejecutará el proceso:** A pesar de que el servicio de energía en la ciudad de Bucaramanga es cada vez más eficiente, no está exento de variaciones de tensión (220 V), como de frecuencia (50Hz) y de la forma de onda (senoidal), afectando el funcionamiento de los equipos electrónicos. Para solucionar estos inconvenientes se diseñaron las Unidades de Potencia Ininterrumpida (UPS). De las cuales existen tres tipos, pero para elegir la más adecuada se debe determinar el nivel de protección de energía que se necesita:

1. UPS de tecnología Off-Line

Adecuada para ambientes que requieren una mínima protección energética. En funcionamiento normal, la carga crítica se alimenta directamente de la tensión de la red (de la compañía eléctrica), por tanto, las posibles variaciones de tensión y frecuencia de la red no son reguladas por este tipo de UPS y son reflejadas directamente en su salida. Cuando las variaciones de tensión y frecuencia de la red se salen de los márgenes de funcionamiento de la UPS, ésta pasa a funcionar con sus baterías, para eliminar las cargas.

2. UPS de tecnología Linea-Interactiva

Permite regulaciones de tensión de grado medio o bajo, mediante elevaciones o reducciones de la tensión de red, en caso necesario, de forma que las cargas críticas están siendo alimentadas con una tensión de red dotada de una mínima relación adicional. Durante las intervenciones de tensión de red, esta UPS usa las baterías para realizar la regulación necesaria. Aunque una UPS Line-Interativa proporciona mejor regulación de tensión que un Off-Line, la vida de la batería es a menudo sacrificada.

3. UPS de tecnología On-Line

Especialmente diseñada para alimentar cargas críticas en equipos que son particularmente sensibles a posibles fluctuaciones de tensión de red. Este tipo de UPS protege contra todo tipo de problemas energéticos y continuamente utiliza la tensión de inversor, que es totalmente aislada de la tensión de red, para alimentar las cargas críticas.

Las UPS expresan sus valores de potencia en Watts y en VA, de estos ninguno de los dos puede ser excedido. Por lo general, los fabricantes solamente publican la potencia en VA de la UPS. Sin embargo, es un estándar en la industria, que su valor en Watts es aproximadamente el 60% del valor en VA, ya que es éste el valor típico del factor de potencia de las cargas. Por lo tanto, como un factor de seguridad, se debe asumir que la potencia en Watts de la UPS es el 60% del valor publicado en VA.

Para determinar la cantidad de equipos que pueden ser alimentados por la

UPS, se debe tener en cuenta que la suma de los consumos individuales no supere la potencia en Watts y en VA especificados para la UPS (es indispensable tener en cuenta el factor de potencia de las cargas). Para optimizar el cálculo y evitar posible sobrecarga de la UPS, se debe realizar una medición con los instrumentos adecuados y así obtener datos exactos de los valores en Watts y VA.

- **Cuándo se ejecutará el proceso**: Al colocar en funcionamiento nuevas salas de cómputo o al existir fallos en el suministro del fluido eléctrico.
- **Lo que se espera que suceda durante la ejecución del proceso:** Las baterías de la UPS soporten el apagón por lo menos el tiempo estimado para alcanzar a guardar la información.
- **Lo que no se espera que suceda:** Que las UPS no soporten el tiempo estimado ante la eventualidad de falla en el fluido eléctrico.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Apagar o desconectar el suministro de electricidad principal de la sala afectada, revisar equipos e informar al coordinador funcional de seguridad informática, revisar tomas, si aún existe la garantía llamar al proveedor de las UPS en caso de daño.
- **Qué criterios indican la ejecución exitosa del proceso:** El soporte adecuado y por el tiempo esperado de las pilas de las UPS que permitan guardar la información en caso de falla en el fluido eléctrico, la ausencia de fallos hardware en equipos.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Luego de solucionar el inconveniente de seguridad, se debe enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Más que con otros procesos, gestión por parte del ejecutivo de Seguridad Informática (Jefe de la D.S.I ante el Consejo de Seguridad Informática para la obtención de recursos).

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Apagar equipos, revisar UPS, llamar a la empresa proveedora de las UPS.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Daños hardware en servidores
Observaciones: Evita – amenaza2.
Daño o falla en alguno de los componentes hardware del equipo (discos duros,

memoria, procesadores, tarjetas de circuitos, fuente, etc.
Tipo Procedimiento (P: Preventivo, C: Correctivo): C
Propósito del procedimiento: • **Qué estándar cumple:** D-1-1.1, D-1-1.2, D-1-1.3, D-1-1.4, D-1-1.5, D-1-1.6, D-1-1.7 • **Cuál es el objetivo del procedimiento:** Corregir daños hardware a equipos servidores.
Alcance del procedimiento: • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a equipos servidores de las salas de cómputo de la D.S.I y en general a toda la red de la UIS y demás campus. • **Qué función se espera que este proceso ejecute**: Corregir daños hardware en equipos servidores. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en hardware de equipos computacionales.

Definición del proceso

- **Introducción al proceso**

▪ **Descripción de lo qué el proceso hace**: Permite cambiar hardware defectuoso a equipos servidores evitando en lo posible afectar la información misma y su disponibilidad.

- **Descripción detallada de:**

▪ **Cómo se ejecutará el proceso:** En la actualidad existen diferentes mecanismos para evitar los retrasos ocasionados por daños en el hardware en los procesos realizados en un servidor. Algunos de estos procesos son:

1. Drives de Cambio Rápido. Los discos del tipo cambio rápido (Hot Swap), brindan la posibilidad de ser removidos del equipo en caliente, es decir, cuando éste se encuentra encendido y sin necesidad de interrumpir la conexión con el sistema operativo. Posibilitando que si alguna parte del servidor llega a fallar, simplemente se inserta el disco en otra máquina en standby idéntica, configurada previamente y lista para poner en línea.
2. Servidores en Standby. Este procedimiento consiste en tener una máquina idéntica de respaldo, lista para poner On Line, cuando por fallas en el hardware del servidor éste se encuentre fuera de servicio.
3. Efectuar periódicamente copias de seguridad de la información contenida en los discos, en los diversos medios de almacenamiento como cintas, CD ROM, e inclusive otros discos duros; de tal forma que si llega a ocurrir un daño en un disco del servidor, éste pueda ser removido en caliente y reemplazado por la copia de seguridad sin ocasionar mayores contratiempos.

▪ **Cuándo se ejecutará el proceso**: Al remover y cambiar alguna parte defectuosa de un servidor.

▪ **Lo que se espera que suceda durante la ejecución del proceso:** Que el equipo esté en lo posible disponible así se tenga que cambiar alguna parte defectuosa en el más breve tiempo.

▪ **Lo que no se espera que suceda:** Que el equipo quede inutilizado por largo tiempo, y que la información quede inaccesible.

▪ **Las acciones que se tomarán si ocurre un hecho imprevisto:** Recurrir a copias de seguridad o respaldo de la información.

▪ **Qué criterios indican la ejecución exitosa del proceso:** Si el servidor continúa en funcionamiento normalmente y en la menor brevedad de tiempo.

▪ **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Luego de solucionar el inconveniente de seguridad, se debe enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática.

▪ **Las interacciones requeridas o esperadas de otros procesos:** Si se tienen máquinas con drives de cambio rápido o máquinas en stand by se espera que los procesos continúen normalmente.

Problemas de los procesos

• **Qué se hará si se presenta un problema en el proceso:** Recurrir a las copias de seguridad.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO: Protección contra elevada temperatura en la sala de servidores **Observaciones: Evita – amenaza3.** Elevada Temperatura en la sala de servidores
Tipo Procedimiento (P: Preventivo, C: Correctivo): P
Propósito del procedimiento: • **Qué estándar cumple:** D-1-1.2, D-1-1.6, D-3-3.1, D-3-3.6 • **Cuál es el objetivo del procedimiento:** Evitar posibles incendios que puedan provocar daños en equipos servidores.
Alcance del procedimiento: • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a equipos servidores de las salas de cómputo de la D.S.I y en general a toda la red de la UIS y demás campus. • **Qué función se espera que este proceso ejecute**: Prevenir incendios que causen daños a equipos servidores. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en hardware de equipos computacionales y equipos de aire acondicionado, especialmente.

Definición del proceso

- **Introducción al proceso**

▪ **Descripción de lo qué el proceso hace**: Permite proteger los equipos servidores de calentamiento excesivo que pueda originar incendios, esto mediante la incorporación de equipos de aire acondicionado (AC).

- **Descripción detallada de:**

▪ **Cómo se ejecutará el proceso:** El aire acondicionado (AC) permite adecuar y controlar la temperatura para el óptimo funcionamiento de los equipos de cómputo, para su instalación se debe tener en cuenta:

- Riesgos

- La instalación del AC es una fuente de incendios.
- Mal funcionamiento del AC ocasiona que el equipo de cómputo se apague.

- Capacidad del equipo de AC

- El AC debe conectarse directamente al generador de electricidad.
- Se presenta disipación térmica a causa de las máquinas y el personal.
- Pérdidas por puertas y ventanas.
- El AC debe ser independiente del aire general.

- Prevenciones

- Para aumentar la seguridad se puede instalar AC de respaldo. En caso que no exista AC de respaldo, se debe contar con una solución de contingencia, por ejemplo ventiladores.
- Alarmas de temperatura y humedad.
- Extintores y detectores de humo.

- Distribución del aire en la sala

- Distribución por dos canales.
- Distribución por techo.

▪ **Cuándo se ejecutará el proceso**: Antes de poner en funcionamiento una sala de cómputo.

▪ **Lo que se espera que suceda durante la ejecución del proceso:** Que el aire acondicionado mantenga unas condiciones de temperaturas en los equipos servidores que evite incendios y por consiguiente indisponibilidad de la información.

▪ **Lo que no se espera que suceda:** Que existan elevadas temperaturas que ocasionen daños a los servidores y por consiguiente información sensible.

▪ **Las acciones que se tomarán si ocurre un hecho imprevisto:** Bajar los tacos o fuentes de energía principales de las salas afectadas. Además de copias de seguridad.

▪ **Qué criterios indican la ejecución exitosa del proceso:** Que los servidores y demás equipos de las salas funcionen adecuadamente.

▪ **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de

Seguridad Informática

- **Las interacciones requeridas o esperadas de otros procesos:** El suministro de energía sea normal.

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Evitar utilizar los equipos mientras se instala dicha protección.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Protección contra Incendio
Observaciones: Evita – amenaza4.
Incendio

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** D-1-1.2, D-1-1.6, D-2-2.8, D-3-3.1, D-3-3.6, D-3-3.7
- **Cuál es el objetivo del procedimiento:** Evitar posibles incendios que puedan provocar daños en equipos servidores.

Alcance del procedimiento:

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a equipos servidores de las salas de cómputo de la D.S.I y en general a toda la red de la UIS y demás campus.
- **Qué función se espera que este proceso ejecute**: Prevenir incendios que causen daños a equipos servidores.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en hardware de equipos computacionales, equipos de aire acondicionado, electricidad, cableado estructurado.

Definición del proceso

- **Introducción al proceso**

▪ **Descripción de lo qué el proceso hace**: Prevenir la posibilidad de ocurrencia de incendios en las salas y por ende de los equipos servidores.

- **Descripción detallada de:**

▪ **Cómo se ejecutará el proceso:** Para evitar o minimizar el impacto de incendio se deben tener en cuenta las siguientes recomendaciones:

- Sala y áreas de almacenamiento impermeables.
- Sistema de drenaje en el piso firme.
- Detectores de fuego alejados del AC.
- Paredes de material incombustible.
- Techo resistente al fuego.
- Canales y aislantes resistentes al fuego.
- Alarmas de incendio.

De acuerdo al origen del fuego se debe usar el tipo de extintor, que puede ser extintor de: H_2O, CO_2, Espuma, Polvo Seco.

▪ **Cuándo se ejecutará el proceso**: Antes de poner en funcionamiento una sala de cómputo, lo mismo que cuando se activen las alarmas en caso de incendio.

▪ **Lo que se espera que suceda durante la ejecución del proceso:** Que las alarmas se activen cuando ocurra un incendio, que los planes de contingencia provoquen una reacción rápida mediante el uso de de extintores, esto incluye simulacros y capacitación a los empleados, además los materiales implantados deben proteger los equipos y salas.

▪ **Lo que no se espera que suceda:** Que las alarmas no funcionen, provocando que el incendio se propague y dañe los equipos de las salas protegidas.

▪ **Las acciones que se tomarán si ocurre un hecho imprevisto:** Bajar los tacos o fuentes de energía principales de las salas afectadas. Desalojar la sala y llamar los bomberos.

▪ **Qué criterios indican la ejecución exitosa del proceso:** Ante simulacros las alarmas se activen en el momento justo, y que el plan de contingencia o reacción se ejecute en el menor tiempo posible evitando el incendio.

▪ **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática

▪ **Las interacciones requeridas o esperadas de otros procesos:** El plan de contingencia ante incendios.

Problemas de los procesos

Qué se hará si se presenta un problema en el proceso: Evacuar el personal, en caso de salirse de las manos la propagación llamar al cuerpo de bomberos

de inmediato. Revisar frecuentemente mediante simulacros el funcionamiento de las alarmas contra incendio.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO: Protección contra Acceso Físico **Observaciones: Evita – amenaza5.** Acceso Físico
Tipo Procedimiento (P: Preventivo, C: Correctivo): P
Propósito del procedimiento: • **Qué estándar cumple:** D-2-2.1, D-2-2.2, D-2-2.3, E-1-1.1, E-1-1.2, E-1-1.3, E-1-1.4, E-1-1.5, E-1-1.6, E-1-1.7, E-1-2.1, E-1-2.2, E-1-2.3, E-1-2.4, E-1-2.5, E-2-2.3 • **Cuál es el objetivo del procedimiento:** Evitar que personal no autorizado accedan a sitios, equipos y como consecuencia a información confidencial de la universidad, pudiendo llegar a efectuarse hasta un atentado terrorista.
Alcance del procedimiento: • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a equipos servidores de las salas de cómputo de la D.S.I y extensible a toda la red de la UIS y demás campus que manejen información sensible para la universidad. • **Qué función se espera que este proceso ejecute**: Impedir el acceso a intrusos o personal no autorizado. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en seguridad de instalaciones físicas, sistemas de video, cableado estructurado.

Definición del proceso

- **Introducción al proceso**

▪ Descripción de lo qué el proceso hace: Impedir el acceso a intrusos o personal no autorizado.

- **Descripción detallada de:**

▪ **Cómo se ejecutará el proceso:** Para prevenir un acceso físico no autorizado a un determinado punto existen diferentes soluciones: analizadores de retina, videocámaras, tarjetas inteligentes o control de las llaves que abren determinada puerta.

Los accesos físicos no autorizados se pueden prevenir siguiendo ciertas normas como:

- Bloquear tomas de red que no se utilizan y que están en lugares apartados.
- Cerrar las puertas con llave al salir de un laboratorio.
- El acceso físico a la sala de servidores debe ser controlado, la puerta de acceso al lugar debe permanecer cerrada para evitar la entrada de personal ajeno y la disipación del aire acondicionado.
- El personal que entra a la sala de servidores debe ser sólo personal autorizado, identificado plenamente. Si se permite el acceso de una persona ajena, esta debe ser registrada y escoltada.
- Cuando se retiren listados o elementos de la sala de servidores, debe quedar un registro del elemento retirado y de la persona que lo retiró, para evitar el extravío y pérdida de listados u otros elementos.

▪ **Cuándo se ejecutará el proceso**: Al ingresar cualquier persona diferente de las autorizadas a la D.S.I, extensible a otras áreas que la universidad considere como críticas para sus procesos.

▪ **Lo que se espera que suceda durante la ejecución del proceso:** Prevenir el ingreso no autorizado a las áreas críticas de la universidad,

▪ **Lo que no se espera que suceda:** Que personal no autorizado acceda libremente y sin control a puntos críticos de la UIS.

▪ **Las acciones que se tomarán si ocurre un hecho imprevisto:** Ubicar posibles puntos desde donde se pudo realizar el acceso no autorizado, también la revisión de los registros de ingreso, lo mismo que el área afectada para ver si falta algo o se encuentra algo sospechoso.

▪ **Qué criterios indican la ejecución exitosa del proceso:** El cumplimiento estricto de estas medidas.

▪ **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática

▪ **Las interacciones requeridas o esperadas de otros procesos:** Coordinación con la empresa de vigilancia que la universidad contrate.

Problemas de los procesos

Qué se hará si se presenta un problema en el proceso: Fortalecer y endurecer las medidas de control.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra debilidad en el sistema de ficheros

Observaciones: Evita – amenaza6.

Sistema de Ficheros

Tipo Procedimiento (P: Preventivo, C: Correctivo): P

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, B-4-4.1, C-1-1.3, H-1-1.1.8, H-1-1.1.10, H-1-1.2.1, H-1-1.2.2, H-1-1.2.3, H-1-1.2.4, H-1-1.2.5, H-1-1.2.6, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** Los permisos otorgados a un archivo determinan quién puede leer, modificar o ejecutar los ficheros almacenados en el sistema Unix. Un error en un permiso puede causar que un usuario pueda modificar todo un disco duro, ejecutar comandos a los que no debería tener derechos o leer archivos e información a la que no debiera tener acceso. Por tal motivo la correcta utilización de los permisos, atributos y otros controles sobre los ficheros son de vital importancia para la seguridad del sistema.

Alcance del procedimiento:

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a aquellos sistemas que posean sistema operativo Unix y extensible a sus diferentes versiones.
- . **Qué función se espera que este proceso ejecute**: Mejorar y propiciar la correcta utilización de los permisos, atributos y otros controles sobre los ficheros.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistemas operativos Unix y sus diferentes versiones como Linux, Solares, Iris entre otros.

Definición del proceso

- **Introducción al proceso:** Un sistema Unix típico consta de tres tipos básicos de archivos: ficheros planos, directorios, y ficheros especiales (dispositivos). La parte del núcleo más visible para los usuarios es el sistema de ficheros; este se encarga de abstraer las propiedades físicas de los diferentes dispositivos para proporcionar una interfaz única de almacenamiento: el archivo. Cada sistema Unix presenta un sistema de archivos nativo. Por ejemplo:

Sistema Unix	**Sistema de Archivos nativo**
Linux	ext2
Solares	Ufs
Iris	Xfs

Los permisos de cada fichero brindan la protección más básica a estos objetos del sistema operativo; describen quién puede acceder a cada uno de ellos, y de que forma puede hacerlo.

- **Descripción detallada de:**
  - **Descripción de lo qué el proceso hace:** La idea de protección utilizada consiste en dividir el universo de usuarios que ve cada fichero en tres clases:
    - La clase u (user), formada únicamente por el dueño del fichero.
    - La clase g (group), formada por todos los usuarios que pertenecen al mismo grupo del dueño.
    - La clase o, formada por el resto del universo.

En Unix un usuario puede pertenecer a más de un grupo pero un fichero sólo puede pertenecer a un grupo. Además se tienen tres formas de acceder a un fichero: lectura, escritura y ejecución. Así los nueve bits de protección de acceso de cada fichero se encuentran divididos en tres grupos de tres bits. Cada grupo de 3 bits indica 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 (r), permiso de ejecución

- **Cómo se ejecutará el proceso:** El root, es el superusuario, es decir, decide qué usuarios pertenecen a qué grupos, los cuales se suelen organizar de acuerdo a razones de trabajo. El administrador de seguridad es el encargado de introducir los datos de los privilegios al sistema. Los privilegios pueden otorgarse individualmente a un usuario o bien a un grupo de usuarios con las mismas características. Un usuario normal tiene la capacidad para autorizar a un tercero sin la intervención del root, siempre que sea el dueño del archivo o directorio sobre el cual se realiza la operación.

Las **Listas de Control de Acceso** (ACLs, Access Control Lists) proporcionan un nivel adicional de seguridad a los ficheros ampliando el clásico esquema de permisos en Unix: mientras que con estos últimos sólo se podía especificar permisos para los tres grupos de usuarios habituales (propietario, grupo y resto), con las ACLs se logran asignar permisos a usuarios o grupos concretos; por ejemplo, se pueden otorgar ciertos permisos a dos usuarios sobre unos ficheros sin necesidad de incluirlos en el mismo grupo o dejarlos en la categoría de otros. Por lo tanto se hace necesario consultar la documentación de los diferentes clones de Unix para detalles concretos sobre el manejo e implementación de las ACLs, mecanismo que se encuentra disponible en la mayoría de sistemas Unix desde hace más de 10 años.

En Solaris, para indicar que una lista de control de acceso otorga permisos no reflejados en los bits rwx se sitúa un símbolo "+" a la derecha de los permisos, cuando se utiliza el comando ls – l se observa:

Pelícano>ls – l /usr/ayuda
-rwx------+ 1 root informix 950 Apr 28 2004 /usr/ayuda

- Las ACLs son adecuadas tanto para incrementar la seguridad como para facilitar ciertas tareas; sin embargo, se pueden convertir en algo también de gran ayuda, para un atacante que desee situar puertas traseras en las máquinas. Un usuario autorizado puede aprovechar un bug del sistema operativo y conseguir privilegios de administrador o root en una máquina; al convertirse en root puede modificar la lista de control de acceso asociada a un archivo importante, por ejemplo, /etc/shadow y crear una nueva entrada que le brinde un permiso total a su login sobre este archivo. Luego de esto borrará todo rastro de su acción. Se tiene entonces un usuario que, aunque los bits rwx no lo indiquen, puede modificar a su gusto un archivo crucial para la seguridad del sistema. Contra esto, poco se puede hacer; simplemente comprobar frecuentemente los listados de todos los ficheros importantes (junto a las ternas de permisos aparece el símbolo "+"), y si se encuentra que un fichero tiene una lista de control que otorga permisos no reflejados en los bits rwx, analizar dicha lista y verificar que todo es correcto. Es muy recomendable programar shellscripts, que automaticen estos procesos e informen en caso de que algo sospechoso se detecte.

- **Cuándo se ejecutará el proceso**: Permanentemente se deben estar revisando los permisos otorgados a los archivos en cuanto a lectura, escritura y ejecución, como también los listados de todos los ficheros importantes.
- **Lo que se espera que suceda durante la ejecución del proceso:** Al descubrir algún usuario con permisos alterados, o si al revisar los listados de todos los ficheros importantes (junto a las ternas de permisos aparece el símbolo "+") se encuentra un fichero que tiene permisos no reflejados en los bits rwx, se debe analizar la lista para verificar que no existe alteración.
- **Lo que no se espera que suceda:** Que personal no autorizado altere los permisos al sistema de ficheros de Unix.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Revisar los listados de todos los ficheros.

- **Qué criterios indican la ejecución exitosa del proceso:** La no alteración de los permisos del sistema de ficheros de Unix.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna.

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Revisar los permisos del sistema de ficheros de Unix.

Excepción del proceso por no aplicabilidad:	**Responsable:**
Exclusivo para sistemas operativos Unix y sus diferentes clones o versiones	

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede surgir al permitir montar y desmontar sistemas de ficheros a los usuarios (generalmente unidades de disquete o CD-ROM)

Observaciones: Evita – amenaza7.

Permitir montar y desmontar sistemas de ficheros a los usuarios (generalmente unidades de disquete o CD-ROM), también puede convertirse en una amenaza de seguridad sino es implantada correctamente.

Tipo Procedimiento (P: Preventivo, C: Correctivo): P

Propósito del procedimiento:

- **Qué estándar cumple:** H-1-1.1.10, H-1-1.2.2, H-1-1.2.3, H-1-1.2.4, H-1-1.2.7

Cuál es el objetivo del procedimiento: Evitar que usuarios sin privilegios puedan montar y desmontar su dispositivo con las opciones por defecto, ya que de no hacerlo es posible que accedan directamente al hardware, por ejemplo, para destruir completamente los discos duros o bloquear la máquina; conseguir privilegios de administrador con la ejecución de un shell o ejecutar un programa almacenado en el dispositivo que él montó.

Alcance del procedimiento:

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a aquellos sistemas que posean sistema operativo Unix y extensible a sus diferentes versiones con algunas variaciones.
- **Qué función se espera que este proceso ejecute**: Evitar que usuarios sin privilegios puedan montar y desmontar dispositivos con las opciones por defecto.

Los conocimientos previos que se necesitan tener para ejecutar el proceso: Conocimientos en sistemas operativos Unix y sus diferentes versiones como Linux, Solares, Irix entre otros.

Definición del proceso

- **Introducción al proceso:** El archivo /etc/fstab (su nombre depende del clon de Unix), enseña qué sistemas de ficheros se montan cuando la máquina arranca y bajo qué nombre de directorio. Dicho montaje se realiza con ciertas opciones tomadas por defecto; como son: rw (se permite tanto la lectura como la escritura), suid (se permite la existencia de ficheros setuidados), dev (se permite la existencia de dispositivos), exec (se permite la ejecución de binarios), auto (el sistema se monta automáticamente al arrancar o al utilizar mount-a), nouser (sólo puede ser montado por el root) y async (la entrada/salida sobre el dispositivo se realiza de forma asíncrona). Estas son las opciones más lógicas para los sistemas de ficheros normales, pero no para los que pueden montar los usuarios. Si se les deja a los usuarios sin privilegios, montar y desmontar su dispositivo con las opciones por defecto, es posible que accesen directamente al hardware, por ejemplo, para destruir completamente los discos duros o bloquear la máquina; conseguir privilegios de administrador con la ejecución de un shell o ejecutar un programa almacenado en el dispositivo que él montó.

- **Descripción de lo qué el proceso hace:** Al arrancar un sistema Unix incorpora diferentes sistemas de ficheros (discos completos, una partición, una unidad de CD-ROM) a la jerarquía de directorios; a este proceso se le denomina montaje, y para efectuarlo generalmente se utiliza la orden mount. Es obligatorio montar al menos un sistema de ficheros durante el arranque, el sistema raíz ("/"), del que se desprenderán todos los demás. Se expresó anteriormente que el archivo /etc/fstab, indica que sistemas de ficheros se montan cuando la máquina arranca y bajo que nombre de directorio, con la importancia de que si alguna de las entradas en el archivo fstab está errada, el sistema no arranca o arranca incorrectamente. Por lo tanto el fichero /etc/fstab debe ser sólo modificable por el root, aunque es adecuado conceder a los usuarios sin privilegios permiso para leer el archivo.

- **Cómo se ejecutará el proceso:** Para permitir a un usuario sin privilegios montar y desmontar un determinado sistema de ficheros, se debe especificar la opción "user" en la entrada correspondiente de fstab, también es conveniente utilizar "noauto" para que el sistema no se monte automáticamente en el arranque de la máquina. Si se permite a un usuario montar una unidad se debe utilizar "nodev", de forma que si en el sistema montado existen ficheros de tipo dispositivo (por ejemplo un archivo que haga referencia a nuestros discos duros) ese fichero sea ignorado, en caso contrario, cualquiera, podría acceder directamente a nuestro hardware, para destruir completamente los discos duros o bloquear toda la máquina. También es importante especificar "nosuid", de forma que se ignore el bit de setuid en cualquier fichero contenido en el sistema que el usuario monta: así se evita que con un shell setuidado en un disco flexible el usuario consiga privilegios de administrador en el sistema. Se puede especificar "noexec", de forma que no pueda ejecutar nada de lo que está en el dispositivo montado. Las opciones (noexec, nosuid y nodev) en Linux se asumen simplemente al indicar "user", pero en otros sistemas Unix quizás no, por lo que no sobra ponerlas explícitamente o consultar el manual en otros

clones de Unix para asegurarse del efecto de cada opción; de esta forma, si queremos que los usuarios puedan montar una unidad de disquete, una entrada correcta en /etc/fstab es la siguiente:

```
Pelicano> grep fd0 /etc/fstab
/dev/fd0 /floppy ext2 user,noauto,nodev,nosuid,noexec
Pelicano>
```

- **Cuándo se ejecutará el proceso**: Permanentemente, pero especialmente al montar el sistema de ficheros del sistema, cuando se define n los privilegios para los usuarios.
- **Lo que se espera que suceda durante la ejecución del proceso:** Que en caso de permitírsele a un usuario no autorizado el montaje del sistema de ficheros no vaya a afectar la información de la universidad.
- **Lo que no se espera que suceda:** Que personal no autorizado altere los discos de nuestro sistema, o ejecute rutinas nocivas, y mucho menos que consiga permisos de administrador del sistema, o que un disco se llene.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Para evitar los problemas que se ocasionan cuando un disco se llena, como son: logs que no se registran, imposibilidad para almacenar información y hasta bloqueo del equipo. Es recomendable montar dispositivos diferentes para todos y cada uno de los directorios sobre los que los usuarios tienen permiso de escritura; esto incluye el padre de sus $HOME, /tmp/ o /var/tmp/. Se puede también establecer un sistema de quotas de disco en la máquina para evitar que un usuario llene el disco y no permita grabar a los demás usuarios.
- **Qué criterios indican la ejecución exitosa del proceso:** La no alteración de los permisos del sistema de ficheros de Unix.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna.

Problemas de los procesos

Qué se hará si se presenta un problema en el proceso: Repetir la operación descrita, revisando el archivo /etc/fstab de Unix.

Excepción del proceso por no aplicabilidad:	**Responsable:**
Exclusivo para sistemas operativos Unix y sus diferentes clones o versiones	

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar los bits setuid y setgid de Unix.

Observaciones: Evita – amenaza8.

Los bits de setuid y setgid proporcionan a Unix una gran flexibilidad, pero

constituyen al mismo tiempo la mayor fuente de ataques internos al sistema (entendiendo por ataques internos aquellos realizados por un usuario autorizado o no, desde la propia máquina, generalmente con el objetivo de aumentar su nivel de privilegio en la misma).

Tipo Procedimiento (P: Preventivo, C: Correctivo): P

Propósito del procedimiento:

- **Qué estándar cumple:** H-1-1.1.10, H-1-1.2.1, H-1-1.2.2, H-1-1.2.3, H-1-1.2.4

Cuál es el objetivo del procedimiento: Impedir que un usuario no autorizado obtenga privilegios sobre el sistema Unix aprovechando debilidades de los bits setuid y setgid

Alcance del procedimiento:

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Aplicables a aquellos sistemas que posean sistema operativo Unix y extensible a sus diferentes versiones con algunas variaciones.
- . **Qué función se espera que este proceso ejecute**: Evitar que usuarios sin privilegios obtengan privilegios sobre el sistema Unix.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistemas operativos Unix y sus diferentes versiones como Linux, Solares, Iris entre otros.

Definición del proceso

- **Introducción al proceso:** Los bits de setuid y setgid proporcionan a Unix una gran flexibilidad, pero constituyen al mismo tiempo la mayor fuente de ataques internos al sistema (entendiendo por ataques internos aquellos realizados por un usuario autorizado o no, desde la propia máquina, generalmente con el objetivo de aumentar su nivel de privilegio en la misma). La consecuencia de activar el bit setuid sobre un fichero implica que todo aquel que ejecute el archivo va a tener durante su ejecución los mismos privilegios que quién lo creó; es decir, si el administrador crea un fichero y lo setuida, todo aquel usuario que lo ejecuta va a disponer, hasta que el programa finalice, de un nivel de privilegio total en el sistema. El archivo se ve de la siguiente manera:

```
>ls –l  /bin/passwd
>-rws r-xr-x    1 root    sys 30552  Jun 25 2005 /bin/passwd
```

Todo lo expresado con relación al bit setuid es aplicable al bit setgid pero a nivel de grupo del fichero en lugar de propietario: en lugar de trabajar con el EUID del propietario, todo usuario que ejecute un programa setgidado tendrá los privilegios del grupo al que pertenece el archivo. Si el fichero es un directorio y no un archivo plano, el bit setgid afecta a los ficheros y subdirectorios que se creen en él: estos tendrán como grupo propietario al mismo que el directorio setgidado, siempre que el proceso que los cree pertenezca a dicho grupo. El archivo se observa de la siguiente manera:

```
> ls –l /bin/passwd
> -rwsr-s r-x   1 root    sys 30552  Jun 25 2005  /bin/passwd
```

- **Descripción de lo qué el proceso hace:** Los sistemas Unix tienen cierto número de ejecutables setuidados y/o setgidados. Cada uno de ellos se ejecuta con los privilegios de quien lo creó, lo que directamente implica que cualquier usuario tiene la capacidad de lanzar tareas que escapen total o parcialmente al control del sistema operativo: se ejecutan en modo privilegiado si es el administrador quien creó los ejecutables. Evidentemente, estas tareas han de estar controladas de forma exhaustiva, ya que si una de ellas se comporta en forma anormal (un simple core dump) puede causar daños irreparables al sistema. Algunos de los archivos setuidados son estrictamente necesarios en Unix, como es el caso de /bin/passwd, la orden para que los usuarios puedan cambiar su contraseña de entrada al sistema, una de sus funciones consiste en modificar el fichero de claves (/etc/passwd o /etc/shadow). Un usuario normal no tiene el nivel de privilegio necesario para hacer esto (es posible que ni siquiera pueda leer el fichero de claves), por lo que frente a este problema parece imprescindible el bit de setuid en el archivo /bin/passwd.

- **Cómo se ejecutará el proceso:** Si falla un programa setuidado ocasionará un grave problema de seguridad para la máquina, ante esta situación se deberá proceder a resetear el bit setuid cuanto antes.

Para el correcto funcionamiento del sistema es necesario que algunos archivos como /bin/passwd tengan activo el bit setuid, pero esto no siempre es así, por ejemplo a un sistema Unix recién instalado la cantidad de ficheros setuidados suele ser mayor de cincuenta; es posible reducir este número a menos de cinco sin afectar el adecuado funcionamiento de la máquina, esta es una de las tareas del administrador sobre un sistema recién instalado: minimizar el número de ficheros setuidados o setgidados. No es adecuado eliminarlos, sino resetear su bit de setuid mediante el comando chmod:

```
Pelicano> ls    -lF    /bin/tar
-r-sr-xr-x   1    root   sys    14  Jun 30    2004    /bin/tar*
Pelicano> chmod u-s /bin/tar
Pelicano> ls    -lF   /bin/tar
-r-xr-xr-x   1    root   sys      14  Jun 30  2004  /bin/tar*
Pelicano>
```

Cuando se instalan nuevas aplicaciones Unix o se actualizan las existentes se debe observar los archivos setuidados que estas aplicaciones instalan por defecto en la máquina, debido a que en algunos archivos ejecutables no se hace necesario este bit activo, por tal motivo, el administrador del sistema, debe resetear el bit de los ficheros que no lo necesiten. Los archivos setuidados no son aplicaciones del sistema ni son aplicaciones añadidas, el hecho de que aparezcan indican en casi el 100% de los casos que el equipo ha sido atacado. Para poder observar los ficheros en algunos de estos bits activos, se puede ejecutar lo siguiente:

```
Pelicano> find  /    \( -perm -4000 –o –perm -2000 \) –type f – print
```

Antes de llamar a exec(), resetear los UIDs y GIDs efectivos. Debido a que uno de los problemas de los programas setuidados es la ejecución de otros programas de manera inesperada; por ejemplo, si el usuario introduce datos desde el teclado, que se han de pasar como argumento a otra aplicación, nada asegura que esos datos sean correctos o coherentes. Es así, que se aconseja resetear el UID y el GID efectivos antes de invocar a exec(), de forma que cualquier ejecución inesperada se realice con el mínimo privilegio necesario; esto también es aplicable a funciones que indirectamente realicen el exec(), como system() o popen().

- **Cuándo se ejecutará el proceso**: Permanentemente, esta es una de las tareas del administrador sobre un sistema recién instalado: minimizar el número de ficheros setuidados o setgidados. No es adecuado eliminarlos, sino resetear su bit de setuid mediante el comando chmod.
- **Lo que se espera que suceda durante la ejecución del proceso:** Minimizar el número de ficheros setuidados o setgidados, ya que con esto se disminuye el riesgo de que un usuario no autorizado adquiera privilegios.
- **Lo que no se espera que suceda:** Que personal no autorizado aumente los privilegios del sistema.

- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Examinar exhaustivamente por parte del administrador el número de ficheros setuidados o setgidados con el objeto de minimizarlos..
- **Qué criterios indican la ejecución exitosa del proceso:** La no alteración de los permisos del sistema de ficheros de Unix.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación descrita, minimizando el número de ficheros setuidados o setgidados, reseteando el bit setuid mediante el comando chmod.

Excepción del proceso por no aplicabilidad:	**Responsable:**
Exclusivo para sistemas operativos Unix y sus diferentes clones o versiones	

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: Daytime: Time of Day, Puerto TCP 13

Observaciones: Evita – amenaza9.

Servicios Disponibles en el Servidor Pelícano: Daytime: Time of Day, Puerto TCP 13

Tipo Procedimiento (P: Preventivo, C: Correctivo): P

Propósito del procedimiento:

- **Qué estándar cumple:** H-1-1.2.7

Cuál es el objetivo del procedimiento: Impedir que un usuario no autorizado obtenga servicios del servidor Pelícano innecesarios, como en este caso Daytime, debido a que un intruso puede obtener información como el estado del reloj del sistema, además de la ubicación geográfica del equipo.

Alcance del procedimiento:

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial los servicios disponibles de dicho servidor, extensible a los demás servidores críticos de la universidad.
- . **Qué función se espera que este proceso ejecute**: Evitar que usuarios sin privilegios puedan obtener el estado del reloj del sistema, además de una ubicación geográfica del equipo.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros.

Definición del proceso

- **Introducción al proceso:** Daytime es un servicio interno de inetd (debido a que no hay un programa externo que lo sirva, por lo tanto inetd se encarga de ello); al recibir una conexión a este puerto, el sistema muestra la fecha y la hora:

```
>telnet pelicano daytime
Trying 192.168.19.6…
Connected to pelicano.uis.edu.co.
Escape character is '^]'.
Mon Jun 4 14:30:23:34 2004
Connection closed by foreign host.
```

- **Descripción de lo qué el proceso hace:** A simple vista este servicio parece no representar peligro para la integridad del sistema, pero una norma de seguridad dice: se debe ofrecer sólo los servicios estrictamente necesarios para el correcto funcionamiento de nuestras máquinas. Como daytime no es un servicio básico, se aconseja cerrarlo; porque la información que proporciona aunque escasa, puede ser empleada por un atacante en el sentido de que le informa el estado del reloj del sistema, brindándole una idea de la ubicación geográfica del equipo.

- **Cómo se ejecutará el proceso:** El servicio Daytime no es básico, por lo tanto lo más recomendable es cerrarlo. El archivo /etc/inetd.conf es aprovechado por el demonio inetd, para brindar la mayoría de los servicios de nuestro equipo hacia el resto de las máquinas, haciendo preciso asegurar su correcta configuración. Cada línea del archivo /etc/inetd.conf le indica a inetd cómo actuar cuando recibe una petición en cierto puerto. Para eliminar un servicio, se debe editar el archivo /etc/inetd.conf, comentar la línea correspondiente poniendo el carácter "#" al inicio de ésta y reiniciar el demonio inetd.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web, ya que sólo se deben permitir los servicios estrictamente necesarios.
- **Lo que se espera que suceda durante la ejecución del proceso:** Desactivar el servicio Daytime.
- **Lo que no se espera que suceda:** Que luego de desactivado el servicio, los usuarios de Pelícano puedan ver el reloj del sistema
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar eliminar el servicio Daytime.
- **Qué criterios indican la ejecución exitosa del proceso:** Que cuando los usuarios soliciten el tiempo del sistema no lo puedan obtener.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al

Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática ▪ **Las interacciones requeridas o esperadas de otros procesos:** Ninguna
Problemas de los procesos • **Qué se hará si se presenta un problema en el proceso:** Repetir la operación descrita y comprobar que el sistema no retorne el tiempo del sistema.

Excepción del proceso por no aplicabilidad: Exclusivo para sistemas operativos Unix y sus diferentes clones o versiones	**Responsable:**

NOMBRE DEL PROCEDIMIENTO: Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: Time: Puerto TCP 37 **Observaciones: Evita – amenaza10.** Servicios Disponibles en el Servidor Pelícano: Time: Puerto TCP 37
Tipo Procedimiento (P: Preventivo, C: Correctivo): P
Propósito del procedimiento: • **Qué estándar cumple:** H-1-1.2.7 • **Cuál es el objetivo del procedimiento:** Impedir que un usuario no autorizado obtenga servicios del servidor Pelícano innecesarios, como en este caso Time, debido a que un intruso puede obtener información como el estado del reloj del sistema, además de la ubicación geográfica del equipo.
Alcance del procedimiento: • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial los servicios disponibles de dicho servidor, extensible a los demás servidores críticos de la universidad. • **Qué función se espera que este proceso ejecute**: Evitar que usuarios sin privilegios puedan obtener el estado del reloj del sistema, además de una ubicación geográfica del equipo. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros.

Definición del proceso

- **Introducción al proceso:** Muestra la fecha y hora del equipo, pero en un formato que no entendible para las personas:

```
>telnet pelicano time
Trying 192.168.19.6...
Connected to pelicano.uis.edu.co.
Escape character is '^]'.
ÂÖ<Connection closed by foreign host.
```

- **Descripción de lo qué el proceso hace:** Este servicio es más útil que daytime: una persona no entiende la información mostrada por time, pero sí una máquina Unix. Se emplea time en un servidor para que las estaciones cliente puedan sincronizar sus relojes con él con comandos como netdate o rdate. Se recomienda cerrar este servicio, aunque existen situaciones en las que un administrador prefiere ofrecer time en varias máquinas que ofrecer daytime.
- **Cómo se ejecutará el proceso:** Si el servicio no es necesario para el correcto funcionamiento del servidor, lo recomendable es cerrarlo. Para lo cual se debe editar el archivo /etc/inetd.conf y anteponer en la línea correspondiente al servicio el carácter "#" al inicio de ésta y reiniciar el demonio inetd.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web, ya que sólo se deben permitir los servicios estrictamente necesarios.
- **Lo que se espera que suceda durante la ejecución del proceso:** Desactivar el servicio Time.
- **Lo que no se espera que suceda:** Que luego de desactivado el servicio, los usuarios de Pelícano puedan ver el reloj del sistema
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar eliminar el servicio Time.
- **Qué criterios indican la ejecución exitosa del proceso:** Que cuando los usuarios soliciten el tiempo del sistema no lo puedan obtener.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación descrita y comprobando que el sistema no retorne el tiempo del sistema.

Excepción del proceso por no aplicabilidad: Exclusivo para sistemas operativos Unix y sus diferentes clones o versiones	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: FTP (File Transfer Protocol): puerto TCP 21

Observaciones: Evita – amenaza11.

Servicios Disponibles en el Servidor Pelícano: FTP (File Transfer Protocol): puerto TCP 21

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** FTP es un protocolo de transferencia de ficheros entre sistemas, el cual permite conectar un equipo cliente a un servidor con el fin de descargar o enviar ficheros. El principal inconveniente de FTP es su diseño, ya que está orientado a ofrecer máxima velocidad en la conexión, pero no seguridad, por lo tanto el objetivo central es contrarrestar esta debilidad de dicho protocolo.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial los servicios disponibles de dicho servidor y más exactamente a FTP, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Como FTP brinda en la conexión máxima velocidad, pero no ofrece seguridad en la transmisión de la información, ya que la transporta en texto claro, se espera corregir este defecto, brindándole seguridad al canal de transmisión.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, protocolo FTP, el paquete SSH y su aplicaciones scp y sftp que vienen incluidas.

Definición del proceso

- **Introducción al proceso:** FTP es un protocolo de transferencia de ficheros entre sistemas, el cual permite conectar un equipo cliente a un servidor con el fin de descargar o enviar ficheros, pero lo efectúa en texto claro.

- **Descripción de lo qué el proceso hace:** Uno de los principales inconvenientes de FTP es su diseño, debido a que está orientado a ofrecer máxima velocidad en la conexión, pero no para ofrecer seguridad; ya que todo intercambio de información que se efectúe, desde el login y el password del usuario en el servidor hasta la transferencia de cualquier archivo se realiza en texto claro, haciendo posible que un atacante pueda capturar tráfico usando un sniffer y conseguir un acceso válido al servidor. Otra amenaza a la privacidad de los datos puede surgir si el atacante captura y reproduce los archivos transferidos. La idea es brindarle un canal seguro a la transmisión mediante aplicaciones adecuadas.
- **Cómo se ejecutará el proceso:** Esta amenaza de FTP es posible contrarrestarla empleando aplicaciones como scp y sftp, incluidas en el paquete SSH, ya que permiten transferir todo el tráfico de ficheros cifrados, resultando un muy buen sustituto de FTP, por lo tanto el servicio se puede cerrar editando /etc/inetd.conf.

Otra medida conveniente es restringir la conexión FTP sólo a usuarios que realmente lo necesiten. Se les debe negar el servicio a usuarios del sistema como root, postmaster, sys,uucp, shutdown, bin, sysadm, daemon, entre otros.

El archivo **/etc/ftpusers** contiene línea por línea los nombres de los usuarios a los que no les está permitida una conexión vía FTP, impidiendo de este modo que atacantes en Internet usen esas cuentas para irrumpir en el sistema capturando las contraseñas de entrada usando un paquete sniffer.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web, ya que sólo se deben permitir los servicios estrictamente necesarios.
- **Lo que se espera que suceda durante la ejecución del proceso:** Obtener canales más seguros para la transmisión de datos.
- **Lo que no se espera que suceda:** Que la transmisión viaje en texto claro, facilitando el ataque a intrusos.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar configurar ya sea las aplicaciones scp y sft de SSH, lo mismo que intentar restringir la conexión FTP a usuarios que realmente lo necesiten.
- **Qué criterios indican la ejecución exitosa del proceso:** Que mediante un sniffer se capture la información y se analice y observe totalmente encriptada..
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al

Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática

- **Las interacciones requeridas o esperadas de otros procesos:** SSH

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: Telnet: puerto TCP 23

Observaciones: Evita – amenaza12.

Servicios Disponibles en el Servidor Pelícano: Telnet: puerto TCP 23

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** El servicio Telnet permite utilizar una máquina como terminal virtual de otra a través de la red, de manera que se establece un canal virtual de comunicaciones parecido pero mucho más inseguro a utilizar una terminal físicamente conectada al servidor. Telnet accede remotamente en modo texto a un equipo en principio potente, permitiendo aprovechar su fortaleza de cálculo sin necesidad de desplazamiento hasta la ubicación de ese servidor, trabajando desde nuestro propio equipo. La versión Unix de telnet está implementada con los programas cliente telnet y el servidor telnetd. Por lo tanto es objetivo de este procedimiento contrarrestar el acceso remoto en modo texto a un equipo.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial los servicios disponibles de dicho servidor y más exactamente a Telnet, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Ofrecer seguridad en la transmisión de la información, ya que la trasporta en texto claro, se espera corregir este defecto, brindándole seguridad al canal de transmisión.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicios Telnet, SSH o SSL-Telnet.

Definición del proceso

- **Introducción al proceso:** El servicio Telnet permite utilizar una máquina como terminal virtual de otra a través de la red, de manera que se establece un canal virtual de comunicaciones parecido pero mucho más inseguro a utilizar una terminal físicamente conectada al servidor. Telnet accede remotamente en modo texto a un equipo en principio potente, permitiendo aprovechar su fortaleza de cálculo sin necesidad de desplazamiento hasta la ubicación de ese servidor, trabajando desde nuestro propio equipo. La versión Unix de telnet está implementada con los programas cliente telnet y el servidor telnetd.

- **Descripción de lo qué el proceso hace:** A pesar de ser Telnet un servicio muy útil, no utiliza ningún tipo de cifrado, transmitiendo todo el tráfico entre equipos en texto claro, facilitando a un atacante con un analizador de red (o un sniffer) capturar el login y el password utilizado en la conexión; permitiendo un acceso total a la máquina destino bajo nuestra identidad.
Los demonios telnetd han presentado frecuentemente problemas de programación; ya que cualquier versión de este demonio que no esté actualizada es una potencial fuente de problemas, por lo que se recomienda conseguir la última versión de telnetd para el Unix particular, principalmente para versiones anteriores a 1997. También pueden afectar este servicio amenazas como es el hecho de que un atacante consiga recuperar una sesión que no ha sido cerrada correctamente, el uso de telnet para determinar qué puertos de un host están abiertos, o la utilización del servicio telnet para averiguar el clon de Unix concreto (versión de kernel incluida) que un servidor utiliza, han hecho famosa la inseguridad de este servicio.

- **Cómo se ejecutará el proceso:** Es aconsejable sustituir el servicio telnet por otras aplicaciones semejantes que emplean cifrado para la transmisión de datos, tales como: SSH o SSL-Telnet, estas aplicaciones exigen además de la parte cliente en nuestro equipo, la parte servidora en la máquina remota escuchando en un puerto determinado, que casi siempre es el puerto TCP 22.
  - **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
  - **Lo que se espera que suceda durante la ejecución del proceso:** Obtener canales más seguros para la transmisión de datos.
  - **Lo que no se espera que suceda:** Que la transmisión viaje en texto claro, facilitando el ataque a intrusos.
  - **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar configurar ya sea las aplicaciones SSH o SSL-Telnet.
  - **Qué criterios indican la ejecución exitosa del proceso:** Que mediante un sniffer se capture la información y se analice y observe totalmente encriptada..
  - **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de

inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática ▪ **Las interacciones requeridas o esperadas de otros procesos:** SSH ó SSL-Telnet
Problemas de los procesos • **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO: Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: SMTP (Simple Mail Transfer Protocol): puerto TCP 25 **Observaciones: Evita – amenaza13.** Servicios Disponibles en el Servidor Pelícano: SMTP (Simple Mail Transfer Protocol): puerto TCP 25
Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C
Propósito del procedimiento: • **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7 • **Cuál es el objetivo del procedimiento:** El servicio SMTP es empleado para transferir correo electrónico entre equipos remotos. Este servicio suele ser efectuado por un demonio denominado sendmail, el cual ha sido fuente de numerosos huecos de seguridad en los sistemas Unix. Este procedimiento pretende contrarrestar las vulnerabilidades que se pueden desencadenar a raíz de este servicio.
Alcance del procedimiento • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente a SMTP, extensible a los demás servidores críticos de la universidad. • **Qué función se espera que este proceso ejecute**: Ofrecer seguridad en la transferencia de correo electrónico entre equipos remotos. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicio SMTP.

Definición del proceso

- **Introducción al proceso:** El servicio SMTP es empleado para transferir correo electrónico entre equipos remotos. Este servicio suele ser efectuado por un demonio denominado sendmail, el cual ha sido fuente de numerosos huecos de seguridad en los sistemas Unix, dentro de las cuales se resaltan debilidades como:

- Facilitar mediante el envío de un correo electrónico formateado de manera especial, que los intrusos informáticos puedan hacerse con el control del servidor de correo. Vulnerabilidad muy delicada porque el atacante no necesita ningún conocimiento específico sobre su objetivo.
- Permitir que un atacante de acuerdo a su habilidad, acceda remotamente como root al sistema objetivo.
- Facilitar a una dirección de correo errónea ejecutar un buffer overflow sobre el servidor.

Sendmail presenta problemas debido a su diseño complicado, su programación en un solo bloque, corre como superusuario y acepta conexiones desde cualquier computador en internet, además posee una gran variedad de comandos, factores que no hacen extraño la presencia de agujeros de seguridad en su código. Ninguna versión de sendmail anteriores a la 8.11.6 es recomendable debido a fallas graves de seguridad. El fichero de configuración principal de sendmail es /etc/sendmail.cf y los comandos VRFY y EXPN también presentan fallos de seguridad por lo tanto deben ser deshabilitados. VRFY permite a alguien hacer telnet al servidor de sendmail con el fin de averiguar si es una dirección válida, facilitando ataques de tipo spam. Además, muchos ataques informáticos a redes comienzan averiguando un nombre de cuenta válida en una máquina.

Ejemplo:

```
>telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 pelicano.uis.edu.co ESMTP Sendmail SGI-8.9.3; Mon, 21 Jun 2004
15:33:25-0400 (EDT)
vrfy root
250 Super-User<root@pelicano.uis.edu.co>
vrfy poncho
550 pepito...User unknown
quit
221 pelicano.uis.edu.co closing connection
Connection closed by foreign host.
```

Otro comando de cuidado es **EXPN,** ya que permite hacer telnet al servidor de sendmail y proporcionar un alias. Este comando proporciona la lista de todas las direcciones de correo que pertenecen al alias y se hace peligroso, debido a que muchas máquinas tienen listas de usuarios, que al ser expandidas permiten obtener los nombres de muchos usuarios, situación que puede ser

aprovechada por un atacante.

- **Descripción de lo qué el proceso hace:** El servicio SMTP puede tener una protección básica al ofrecer el servicio sendmail desde inetd, en lugar de hacerlo como un demonio independiente, con el fin de poder restringir el acceso al mismo mediante TCP Wrappers. Generalmente las organizaciones tienen un servidor de correo principal que se ocupa de recoger el correo para todas las direcciones "*@*uis.edu.co"; los demás equipos recibirán correo sólo desde este servidor. Por lo tanto, si sendmail sólo recibe correo válido desde una máquina, se debe configurar para que sólo acepte peticiones desde ella: en lugar de lanzar el demonio al arrancar el sistema, en uno de los scripts de /etc/rc.d/ o similar, se servirá desde inetd.

- **Cómo se ejecutará el proceso:** Para esto se hace necesario cambiar el script correspondiente para que sendmail no se lance como demonio en el arranque: en lugar de invocarlo como **"sendmail –bd –q15m"** se hace como "**sendmail –q15m**". Además, se debe identificar el servicio en /etc/services, con una línea como la siguiente: **smtp 25/tcp mail**. Después de reconocer el servicio, es necesario añadir una línea en **/etc/inetd.conf** indicando como ha de ejecutar sendmail cuando inetd reciba una petición en el puerto 25; dicha línea es similar a la siguiente: **smtp stream tcp nowait root /usr/sbin/tcpd sendmail –bs.**

Al aplicar estos cambios se hace posible controlar el acceso al servicio smtp mediante TCP Wrappers; para el caso particular de la UIS, el servidor de correo principal se denomina condor.uis.edu.co, y sólo desde esta máquina nos pueden enviar correo, si se incluye la siguiente línea:

/etc/hosts.allow:
sendmail: condor.uis.edu.co

A los demás sistemas no se les debe autorizar la conexión a este puerto; incluyendo también a la máquina local, ya que: para un correcto funcionamiento del sistema de correo, ni siquiera hace falta que localhost tenga permiso para acceder a su puerto 25. Esta medida es aplicable a sistemas que reciben correo de un único mailer. Para configurar el propio mailer de la organización, que casi siempre recibe correo de un número indeterminado de máquinas, no puede bloquearse el acceso a su sendmail de esta forma. Sin embargo se pueden tener en cuenta unas medidas de seguridad simples tales como: la realización de una consulta inversa a DNS con el fin de asegurar que sólo máquinas registradas envían correo o no permitir que nuestro sistema reenvíe correo que no provenga de direcciones registradas bajo su dominio. Las anteriores medidas son necesarias en la configuración de los sistemas de cualquier entidad para evitar problemas de spam y mail bombing.

Para recibir correo electrónico usando sendmail es conveniente tomar ciertas medidas de seguridad:

1. Comprobar que sendmail no soporta los comandos debug, wiz, o kill. Se pueden probar con las siguientes órdenes:

```
>telnet localhost smtp
Trying 127.0.0.1…
Connected to localhost.
Escape character is '^]'.
220 pelicano.uis.edu.co ESMTP Sendmail SGI-8.9.3/8.9.3; Mon, 19 Jun
2004 15:14:14-
0400 (EDT)
wiz
500 Command unrecognized: "wiz"
kill
500 Command unrecognized: "kill"
debug
500 Command unrecognized: "debug"
quit
221 pelicano.uis.edu.co closing connection
Connection closed by foreign host.
>
```

En caso de que sendmail responda a los comandos debug o wiz con un mensaje cualquiera diferente a "command unrecognized", se debe reemplazar la versión existente de sendmail.

2. Borrar el alias "decode" del archivo **aliases**. La línea se ve así:

Decode: "|/usr/bin/uudecode"

El alias decode permite que el correo sea enviado directamente al programa uudecode, pero se ha comprobado que esta capacidad es un hueco en la seguridad, por lo tanto se debe revisar con sumo cuidado cada alias que apunte a un archivo o programa en vez de a una cuenta de usuario. Después de realizar los cambios en el archivo aliases se debe correr **newaliases.**

3. Revisar que el archivo aliases esté protegido de modificaciones de usuarios diferentes al administrador del sistema. En caso contrario, los usuarios podrían adicionar nuevos alias para correr programas, redireccionar emails, entre otros. Si la versión de sendmail crea los archivos aliases.dir y aliases.pag estos archivos también deben ser protegidos.

4. Compruebe que el password "wizard" se encuentra desactivado en el archivo sendmail.cf. En caso contrario, si una persona conoce el password del wizard podrá conectarse al demonio sendmail de la máquina e iniciar la ejecución de un shell en ella. Si esta característica esta disponible en la versión de sendmail, la línea de password comienza con las letras OW. Si se encuentra una línea de estas características, se debe cambiar a:

Disallow wizard password:
OW*

5. Deshabilitar los comandos VRFY y EXPN. Debe encontrar en /etc/sendmail.cf la línea:

O PrivacyOptions=

Para deshabilitar EXPN y VRFY, cambie la línea de la siguiente forma:

O PrivacyOptions=noexpn novrfy

Para mayor privacidad:

O PrivacyOptions=goaway

Ahora debe recargar la configuración de sendmail, iniciándolo nuevamente. Para probar que funciona, puede hacer telnet a localhost puerto 25 y ejecutar el comando vrfy "username".

6. Compruebe que tiene la versión más reciente de sendmail instalada en la máquina. En los sitios www.sendmail.com puede realizar actualizaciones tan pronto como las vulnerabilidades sean publicadas.

Otras alternativas para sendmail consisten en vez de tener un solo programa que recibe y entrega correo, tener dos programas diferentes: el Firewall Toolkit de Trusted Information Systems[27] contiene un programa llamado smap, (sendmail wrapper) que acepta conexiones SMTP desde el exterior. El TIS Firewall Toolkit elimina muchos de los problemas de seguridad de sendmail porque llega al centro del problema y rompe la conexión entre el sendmail y el mundo exterior. En lugar de tener un solo programa de SUID (sendmail) escuchando por conexiones en el puerto 25, implementando un complejo conjunto de instrucciones y entregando correo a los buzones de los usuarios; el paquete TIS emplea un par de programas (smap, smapd), los cuales son empleados uno para aceptar correo de la red y otro para entregarlo.

Smap. Este programa recibe mensajes de la red y los aloja dentro de un directorio especial para su futura entrega. Se ejecuta en un filesystem chroot especialmente diseñado, desde el cual no puede dañar al resto del sistema operativo. El demonio está diseñado para ser invocado desde inetd y salir cuando se termine la sesión de reparto del correo.

Smapd. Este programa revisa periódicamente el directorio donde el smap entrega el correo, cuando encuentra mensajes terminados, los entrega al buzón de correo del usuario apropiado usando el sendmail u otro programa. El

[27] Trusted Information Systems es una compañía que desarrolla y vende una variedad de productos y servicios de seguridad. El Firewall Toolkit está disponible para la comunidad UNIX y es para uso libre.

TIS Firewall Toolkit guarda la configuración y la información de permisos en un solo archivo generalmente /usr/local/etc/netperm-table, el cual debe ser escribible solamente por el superusuario. Para mayor seguridad sus permisos deben fijarse a 600. El TIS Firewall Toolkit se puede obtener desde el ftp://ftp.tis.com/pub/firewalls/toolkit/ usando FTP anonymous.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Transmisión de correo electrónico sin problemas.
- **Lo que no se espera que suceda:** Que los intrusos informáticos puedan hacerse con el control del servidor de correo, vulnerabilidad muy delicada porque el atacante no necesita ningún conocimiento específico sobre su objetivo. Que un atacante de acuerdo a su habilidad, acceda remotamente como root al sistema objetivo. Facilitar a una dirección de correo errónea ejecutar un buffer overflow sobre el servidor.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar los agujeros de seguridad.
- **Qué criterios indican la ejecución exitosa del proceso:** Que no existan inconvenientes en la transmisión de correo electrónico, ni anomalías en el servidor de correo.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Con herramientas como TCP Wrappers, smap y smapd.

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: Finger Puerto TCP 79
Observaciones: Evita – amenaza14.
Servicios Disponibles en el Servidor Pelícano: Finger Puerto TCP 79

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** Finger es un protocolo que proporciona información muy completa de los usuarios de una máquina, estén

o no conectados en el momento de acceder al servicio. La información suministrada por finger es de mucha utilidad para un atacante (nombres de usuario, hábitos de conexión, cuentas inactivas, directorio HOME del usuario, número telefónico de la oficina, entre otros) y puede ser usada como base para un ataque de ingeniería social contra los usuarios o contra el propio administrador del sistema, por lo tanto es conveniente tomar medidas para restringir dicho servicio.
Alcance del procedimiento • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente al servicio Finger, extensible a los demás servidores críticos de la universidad. • **Qué función se espera que este proceso ejecute**: Restringir el servicio Finger. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicio Finger.

Definición del proceso

- **Introducción al proceso:** Finger es un protocolo que proporciona información muy completa de los usuarios de una máquina, estén o no conectados en el momento de acceder al servicio. Finger puede utilizarse de dos formas: dándole como argumento el nombre de máquina precedido del símbolo "@" o el nombre de un usuario seguido de "@".

```
Condor> finger @pelicano
```

Finger mostrará datos generales de los usuarios que se encuentren conectados en ese momento a la máquina: nombre de usuario, nombre completo, tiempo de login, número telefónico de la oficina (asumiendo que esta información está almacenada en el archivo /etc/passwd).

```
Condor> finger usuariox@pelicano
```

Finger busca en etc/passwd e informa en detalle acerca del usuario o los usuarios cuyos apellidos, nombres o username coincidan con el parámetro especificado, estén o no conectados.

- **Descripción de lo qué el proceso hace:** La información suministrada por finger es de mucha utilidad para un atacante (nombres de usuario, hábitos de conexión, cuentas inactivas, directorio HOME del usuario, número telefónico de la oficina, entre otros) y puede ser usada como base para un ataque de ingeniería social contra los usuarios o contra el propio administrador del sistema, situación que este procedimiento tratará de impedir.
- **Cómo se ejecutará el proceso:** Es básico para la integridad de los servidores inhabilitar este servicio. Hay dos formas de hacerlo:

- Remover o comentar la línea del servicio finger en el archivo /etc/inetd.conf. Esta modificación provoca que al hacer finger sobre la máquina, se reciba el error "Connection refused". El hecho de deshabilitar finger de este modo puede provocar problemas para tratar de determinar direcciones de correo o números de teléfono, ocasionando algunos inconvenientes a quienes traten de acceder el servidor.

- Reemplazar el servicio finger con un shell script que muestre o imprima un mensaje orientando a los usuarios acerca de cómo contactar su sitio. Por ejemplo:

```
#!/bin/sh
#
/bin/cat<<'XX'
Este es el servidor de Bases de Datos Pelicano. Para solicitar
información sobre algún Sistema de información, por favor comuníquese
a la extensión # # # #.
Gracias
XX
```

exit 0

Luego almacene el script en un archivo ejecutable, tal como /usr/local/etc/no_finger. Posteriormente en el archivo /etc/inetd.conf, reemplace la entrada normal de finger con una línea como esta:

finger stream tcp nowait nobody/usr/local/etc/no_finger no_finger

Reinicie inetd

Otra alternativa para finger, esta disponible mediante el servicio ph (phone book), el cual permite almacenar información dentro de una base de datos y especificar cuáles datos deben ser retornados en consultas realizadas desde dentro y fuera de la red. El servidor ph puede descargarse de la dirección: ftp://vixen.cso.uiuc.edu/pub/ph.tar.gz.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilite el servicio finger.
- **Lo que no se espera que suceda:** Que el servicio finger continúe funcionando mostrando información importante para un intruso.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar el servicio finger.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar el servicio finger este no responda.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad:
Ninguna

Problemas de los procesos
Qué se hará si se presenta un problema en el proceso: Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: rexec: Puerto TCP 512

Observaciones: Evita – amenaza15.

Servicios Disponibles en el Servidor Pelícano: rexec: Puerto TCP 512

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** Unix posee los servicios r * que son herramientas con una parte cliente y una servidora que se encargan de la conexión remota entre máquinas, especialmente para servicios de terminal remota y también transferencia de ficheros. Las componentes clientes son rsh, rlogin y rcp, mientras que las servidoras son demonios como rexecd, rshd o rlogind, los cuales pueden presentar inconvenientes que este procedimiento pretende controlar.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente al servicio rexec, extensible a los demás servidores web críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Restringir el servicio rexec.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicio rexec.

Definición del proceso

- **Introducción al proceso:** Unix posee los servicios r - * que son herramientas con una parte cliente y una servidora que se encargan de la conexión remota entre máquinas, especialmente para servicios de terminal remota y también transferencia de ficheros.

- **Descripción de lo qué el proceso hace:** Las componentes clientes son rsh, rlogin y rcp, mientras que las servidoras son demonios como rexecd, rshd o rlogind, los cuales pueden presentar inconvenientes tales como:
rexecd. Es un demonio de ejecución remota /usr/sbin/rexecd que le permite al usuario la ejecución de comandos sobre otros equipos sin necesidad de loguearse en ellos. El problema surge cuando el cliente abre una conexión y transmite un mensaje que especifique tanto el username, el password y el nombre del comando a ejecutar. Como rexecd necesita que el password sea transmitido por la red, este puede ser capturado por un sniffer como también puede ocurrir con un telnet.

Es conveniente resaltar que rexecd emite mensajes de error diferentes para username inválidos y password errados diferentes a telnet. Si el username resulta inválido, rexecd retorna el mensaje de error "login incorrecto". Si el username es correcto y el password es erróneo devuelve un mensaje de error "password incorrecto". Esta situación pudiera provocar que un atacante se aprovechara de rexecd para adivinar passwords partiendo de usuarios válidos.

- **Cómo se ejecutará el proceso:** Debido a que rexec no emplea mecanismos de máquinas fiables puede ser usado por cualquier host en la red. Por lo tanto si no es requerido, se recomienda inhabilitarlo en /etc/inetd.conf.
- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilite el servicio rexec.
- **Lo que no se espera que suceda:** Que el servicio rexec continúe funcionando.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar el servicio rexec.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar el servicio rexec este no responda.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

Qué se hará si se presenta un problema en el proceso: Repetir la operación

anteriormente descrita.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: rlogin: Puerto TCP 513 y rsh: Puerto TCP 514

Observaciones: Evita – amenaza16.

Servicios Disponibles en el Servidor Pelícano: rlogin: Puerto TCP 513 y rsh: Puerto TCP 514

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7

Cuál es el objetivo del procedimiento: rlogin se emplea como terminal virtual de un sistema Unix, de manera muy similar a telnet; donde rlogin es el programa cliente y rlogind es el servidor. Así mismo, rsh es utilizado para ejecutar comandos en una máquina remota sin necesidad de acceder a ella; rsh es el cliente y rshd es el servidor. Tanto rlogin como rsh están diseñados para comunicación sólo entre sistemas Unix Berkeley. Los usuarios que deseen comunicarse entre Unix y TOPS, VMS, u otra clase de sistemas deben usar el protocolo telnet, no el protocolo rlogin. Los servicios r^{-*} evitan el tránsito de contraseñas por la red, mediante el concepto de "máquinas fiables" y "usuarios fiables" donde cualquier usuario, puede hacer uso de los recursos de una máquina remota sin necesidad de una clave si su conexión proviene de una máquina fiable o si su nombre de usuario es fiable, pero esta solución derivó problemas de seguridad que son los que este procedimiento busca controlar.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente a los servicios rlogin: Puerto TCP 513 y rsh: Puerto TCP 514, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Restringir los servicios rlogin: Puerto TCP 513 y rsh: Puerto TCP 514.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicios rlogin: Puerto TCP 513 y rsh: Puerto TCP 514, máquinas fiables.

Definición del proceso

- **Introducción al proceso:** Los servicios r-* evitan el tránsito de contraseñas por la red, y fue conseguido por los diseñadores del sistema de red de Unix BSD mediante la idea de "máquinas fiables" y "usuarios fiables" donde cualquier usuario, puede hacer uso de los recursos de una máquina remota sin necesidad de una clave si su conexión proviene de una máquina fiable o si su nombre de usuario es fiable.

Es posible considerar una máquina fiable de dos formas:

3. Si su nombre (el de la máquina) se encuentra en el directorio /etc/hosts.equiv.
4. Si su nombre (el de la máquina) se encuentra en un fichero denominado .rhosts situado en el $HOME del usuario.

En el primer caso, cualquier usuario (excepto el root) del sistema remoto (y fiable) puede acceder al equipo bajo el mismo login que tiene en el primero, sin necesidad de claves. En el segundo caso, empleando los ficheros .rhosts, cualquier usuario del sistema remoto podrá conectar al nuestro pero sólo bajo el nombre de usuario en cuyo $HOME se encuentra el archivo.

El concepto de usuarios fiables es el mismo que el asociado al de máquinas fiables, pero aplicado a nombres de usuario en lugar de nombres de máquina. Los nombres de usuario pueden indicarsen tanto en /etc/hosts.equiv como en los archivos .rhosts; no obstante, la primera opción no es apropiada debido a que permite al usuario fiable del sistema remoto acceder sin contraseña a cualquier cuenta de nuestra máquina. Por lo tanto para crear usuarios fiables de sistemas remotos, es necesario hacerlo en los archivos .rhosts.

- **Descripción de lo qué el proceso hace:** Las relaciones de confianza entre equipos Unix suelen ser muy útiles y cómodas, pero paralelamente son muy peligrosas: ya que si se confía plenamente en sistemas remotos, de llegar a comprometerse su seguridad, también se afectaría la seguridad de otros equipos. Las máquinas fiables se deben reducir a equipos de la misma organización, y administrados por la misma persona; también, es necesario tener presente que al tener habilitados los servicios r* cualquier usuario puede establecer relaciones de confianza. Así mismo, es necesario chequear los directorios $HOME en busca de ficheros .rhosts; y seguir la estrategia de muchos administradores que prefieren no complicarse buscando estos ficheros, y configurar sus sistemas para que en cada $HOME exista un fichero con este nombre, propiedad de root y con modo 000, evitando de esta de esta forma que los usuarios no tengan ocasión de otorgar confianza a sistemas remotos.

Las relaciones de confianza son transitivas, lo cual quiere decir que si una máquina confía en otra, lo hace también en todas en las que confía ella. Así, se crean anillos de confianza entre máquinas. El mecanismo de máquinas fiables usa direccionamiento IP para autenticación por lo cual es vulnerable a ataques por IP spoofing y ataques DNS. Si un intruso consigue hacer pasar su equipo

por uno de los confiables, automáticamente ha conseguido acceso (casi ilimitado) al resto de las máquinas.

- **Cómo se ejecutará el proceso:** Todos los comandos r* (rlogin, rsh, rcp), deben ser desactivados de no ser requeridos, debido a que se exponen las contraseñas al viajar sobre la red, aumentando el riesgo de sufrir ataques de tipo sniffing y spoofing.

∗ De requerirse la utilización de estos comandos, se debe tener en cuenta:

- Contemplar la posibilidad de reemplazar la funcionalidad r* con utilidades más seguras, por ejemplo ssh y scp. Ssh ampliamente superior a rsh, telnet, etc. Debido a que encripta las contraseñas y todos los datos transmitidos durante la sesión.
- No permitir el uso de $HOME/.rhosts.

Revisar que no existe el archivo .rhosts en el directorio HOME de ningún usuario, debido a que estos archivos representan un mayor riesgo de seguridad que el fichero /etc/hosts.equiv, porque pueden ser creados por el usuario. Usar el cron periódicamente, para detectar la existencia de archivos $HOME/.rhosts y eliminarlos del sistema. Es conveniente anotar que los usuarios deben ser informados sobre este proceso de auditoría ejecutado regularmente sobre el sistema.

∗ De ser necesario tener tales archivos entonces se debe asegurar de:

- No debe tener el símbolo "-" como primer carácter en este archivo, o el símbolo "+" en ninguna de sus líneas, debido a que estos pueden permitir el acceso de usuarios no autorizados al sistema.
- Establezca los permisos sobre el archivo a 600.
- Utilizar los hostnames completamente definidos (es decir hostname.dominio.au).
- Especifique en el archivo los nombres de los usuarios confiables.

∗ De no requerirse el uso de los comandos r* o no desearse establecer "máquinas confiables", se recomienda remover de su sistema el archivo /etc/hosts.equiv. De ser necesario usar este archivo se recomienda:
- Mantener sólo un pequeño número de hosts confiables.
- Especificar en el archivo los hosts para los cuales desea permitir el uso de comandos r*.
- Confiar sólo en máquinas dentro de su dominio o bajo su administración.
- Revisar que el archivo no tenga como entrada el caracter "+" en ninguna línea, el signo + tiene el efecto de declarar a cada host confiable. Esta línea es el mayor hueco de seguridad, porque los hosts fuera de la red local (sobre los cuáles el administrador del sistema no tiene control) no deben ser nunca confiables.
- Establecer los permisos sobre el archivo a 600.
- Revisar que el dueño del archivo es el root.
- Chequear el archivo después de la instalación de cada parche sobre el

sistema operativo.

∗ Utilizar versiones más seguras de los comandos de r* para los casos en donde hay una necesidad específica. El paquete **logdaemon** de Wietse Venema contiene una versión más segura de los demonios del comando r* (rsh,rlogin). Estas versiones se pueden configurar para consultar solamente /etc/hosts.equiv y no $HOME/.rhosts. Hay también una opción para inhabilitar el uso de comodines ("+") y de archivos .rhosts del usuario. Logdaemon está disponible vía FTP anónimo desde: ftp://ftp.porcupine.org/pub/security/

∗ Filtrar los puertos TCP 512, 513 y 514 en el router de la red para prevenir el acceso a ellos externamente. Para limitar el acceso a ellos desde dentro de la red, estos comandos deben ser deshabilitados completamente o restringidos a ciertos hosts configurando los archivos hosts.allow y hosts.deny.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilitar los servicios rlogin: Puerto TCP 513 y rsh: Puerto TCP 514.
- **Lo que no se espera que suceda:** Que los servicios continúen activos.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar los servicios.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar los servicios estos no respondan.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: NFS (Network File System): Puerto TCP 2049
Observaciones: Evita – amenaza17.
Servicios Disponibles en el Servidor Pelícano: NFS (Network File System): Puerto TCP 2049

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7

Cuál es el objetivo del procedimiento: NFS es uno de los servicios RPC[28] más ampliamente usados. NFS se encarga que usuarios de una red puedan acceder a archivos almacenados en un servidor. Dicho servicio presenta implicaciones de seguridad tanto para el servidor NFS como para el cliente NFS, por lo tanto este procedimiento pretende hacerle contrapeso a las debilidades presentadas en este servicio.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente a los servicios NFS (Network File System): Puerto TCP 2049, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Restringir los servicios NFS (Network File System): Puerto TCP 2049.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicios NFS (Network File System): Puerto TCP 2049

[28] RPC Remote Procedure Call. Mecanismo que le permite a un programa que está corriendo en un computador ejecutar una función que está corriendo en otro computador. Facilita la creación de redes basadas en programas cliente/servidor: los clientes y el servidor se comunican entre ellos usando RPC.

Definición del proceso

- **Introducción al proceso:** NFS se encarga que usuarios de una red puedan acceder a archivos almacenados en un servidor. Dicho servicio presenta implicaciones de seguridad tanto para el servidor NFS como para el cliente NFS, como las siguientes:

- Acceso Cliente: NFS debe ser configurado para que sólo determinados clientes o hosts en la red puedan montar sistemas de archivos en el servidor. Varias versiones de UNIX, como IRIX de SGI usan el archivo /etc/exports para designar cuáles clientes pueden montar sistemas de archivos y los permisos concedidos.

- Autenticación de Usuario: NFS debe ser configurado para que los usuarios puedan acceder y modificar sólo los archivos a los cuales se les ha otorgado el privilegio de hacerlo.

- Eavesdropping y spoofing de datos. NFS no protege la información de la red de este tipo de ataques, ya que el sistema primario que NFS usa para autenticación de servidores está basado en direcciones IP y hostnames. Además como los paquetes NFS no viajan encriptados, puede suceder que un atacante logre engañar (spoof) un cliente NFS haciéndose pasar como un servidor NFS o cambiar los datos que viajan entre el servidor y el cliente. De este modo el intruso puede forzar a una máquina cliente a correr cualquier ejecutable montado en un NFS. Lo cual le daría al atacante el completo control sobre una máquina NFS cliente.

- **Descripción de lo qué el proceso hace:** Filtrar el acceso al servicio NFS (Network File System): Puerto TCP 2049.

- **Cómo se ejecutará el proceso:** El empleo de NFS, implica también confiar en la seguridad del servidor NFS para mantener la integridad de los archivos montados. Es posible mejorar la seguridad de NFS tomando al menos las siguientes medidas básicas:

- Filtrar el tráfico NFS en el router. Especialmente el puerto 111 TCP/UDP y el puerto 2049 TCP/UDP, con el fin de prevenir el acceso de máquinas que no pertenezcan a la LAN de la organización a sistemas de archivos exportados en sus equipos.
- Aplicar todos los parches disponibles, pues es bien conocido que NFS ha tenido numerosas vulnerabilidades de seguridad.
- Si no se necesita inhabilite NFS.
- Activar el monitoreo de puertos NFS mediante el cambio de la variable nfs_portmon a 1. Esto implica que las llamadas para montar un sistema de archivos serán aceptadas de puertos menores que 1024 solamente, incrementando con esta maniobra seguridad.
- Si no se está seguro de necesitar exportar un sistema, no se debe hacer. En caso de ser necesario utilice /etc/exports o /etc/dfs/dfstab para exportar solamente los sistemas de ficheros que necesita exportar un sistema.

- No permita que el archivo a exportar contenga una entrada localhost.
- Exportar solamente a hostnames completamente definidos, es decir, aquellos con dirección completa de la máquina “nombremaquina.dominio.au” y nunca la abrevie a “nombremáquina”.
- Tenga cuidado de no exportar sistemas de archivos a todo el mundo, para esto utilice la opción access=hosts.domainname.au o su equivalente en /etc/exports.
- Exporte sistemas de archivos de sólo lectura (-ro) siempre que sea posible.
- Utilice el comando showmount –e para comprobar que está exportando únicamente los sistemas de archivos que desea exportar a los host especificados.
- Instaure los permisos de etc/exports a 644.
- Revise que el dueño de /etc/exports es el root.
- Cerciórese al ejecutar un portmapper o rpcbind que estos no remitan peticiones de montaje de clientes, ya que un cliente NFS malicioso puede solicitar al demonio portmapper del servidor, que reenvíe la petición al demonio mount; procesando la petición como si ésta viniera directamente del portmapper, por lo tanto de llegarse a montar el sistema de archivos este otorgaría permisos al cliente no autorizado sobre él.
- No se debe olvidar que los cambios sobre /etcexports tomarán efecto sólo después que corra /usr/etc/exportsfs o su equivalente.
- Puede revisar la implementación de NFS con el programa NFSBug, el cual permite explorar los huecos de seguridad conocidos para NFS. Se encuentra disponible en: ftp://ftp.cs.vu.nl/pub/leendert/nfsbug.shar.
- Restringa el uso de NFS a sólo máquinas en las cuales los sistemas de archivos son exportados, y limite el número de sistemas de archivos que cada cliente monta.
- Remueva el permiso de escritura para el grupo, de los archivos y directorios exportados.
- No exporte los ejecutables propios del servidor (/bin,/usr/bin, /etc.).
- No exporte directorios HOME de usuarios.
- No permita a los usuarios loguearse dentro del servidor.
- Si la opción está disponible utilice NFS Seguro en los archivos exportados y en las peticiones del montaje, ya que emplea autenticación AUTH_DES RPC en vez de AUTH_UNIX. NFS Seguro obliga a los usuarios a descifrar una clave especial almacenada en el servidor NIS o NIS+ antes de que el sistema de archivos NFS le permita al usuario accesar sus archivos. Para activar NFS Seguro, debe especificar la opción segura en el servidor NFS (en los archivos exports o dfstab) y en el cliente (en los archivos /etc/fstab o /etc/vfstab).

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web, pero si no se ha efectuado se puede efectuar en cualquier momento.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilitar el servicio NFS (Network File System): Puerto TCP 2049.
- **Lo que no se espera que suceda:** Que el servicio NFS continúe activo.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar el servicio.

- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar el servicio este no responda.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: RPC (SUN Remote Procedure Call) puerto UDP 111.

Observaciones: Evita – amenaza18.

Servicios Disponibles en el Servidor Pelícano: RPC (SUN Remote Procedure Call) puerto UDP 111

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** RPC es otra forma de ofrecer servicios al igual que inetd o los demonios independientes lanzados al arrancar el sistema. El funcionamiento básico RPC radica en la existencia de un programa denominado portmap, rpcbind, rpc.pormap (su nombre depende del clon de Unix) que los servidores RPC utilizan para registrarse, de tal forma que cuando un cliente desea utilizar estos servicios, en lugar de conectar a un puerto determinado donde se encuentre el servicio lo hace al puerto del portmapper, que le facilitará la ubicación exacta del servicio solicitado. Portmapper es aprovechado para asignar dinámicamente los puertos TCP y UDP usados para llamados de procedimiento remoto, es muy parecido al demonio inetd, en el sentido de que media en las comunicaciones entre clientes y servidores de red, los cuales podrían tener problemas de seguridad, objetivo al cual apunta este procedimiento.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente a los servicios RPC (SUN Remote Procedure Call) puerto UDP 111, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Restringir los servicios

RPC (SUN Remote Procedure Call) puerto UDP 111.

- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicio RPC (SUN Remote Procedure Call) puerto UDP 111.

Definición del proceso

- **Introducción al proceso:** RPC es otra forma de ofrecer servicios al igual que inetd o los demonios independientes lanzados al arrancar el sistema; original de SUN Microsystems pero en la actualidad está implementado también por OSF (Open Software Foundation) en su DCE (Distributed Computing Environment) y por OMG (Open Management Group) en CORBA (Common Object Request Broker Architecture). El funcionamiento básico RPC radica en la existencia de un programa denominado portmap, rpcbind, rpc.pormap (su nombre depende del clon de Unix) que los servidores RPC utilizan para registrarse, de tal forma que cuando un cliente desea utilizar esos servicios, en lugar de conectar a un puerto determinado donde se encuentre el servicio lo hace al puerto del portmapper, que le facilitará la ubicación exacta del servicio solicitado. Portmapper es aprovechado para asignar dinámicamente los puertos TCP y UDP usados para llamados de procedimiento remoto, es muy parecido al demonio inetd, en el sentido de que media en las comunicaciones entre clientes y servidores de red, los cuales podrían tener problemas de seguridad.

- **Descripción de lo qué el proceso hace:** Filtrar el acceso al servicio RPC (SUN Remote Procedure Call) puerto UDP. El portmapper estándar de UNIX, delega el manejo de la seguridad a los servidores, permitiendo además que cualquier cliente de la red se comunique con cualquier servidor RPC, resultando los mecanismos RPC generalmente muy complejos, y difíciles para garantizar la seguridad en ellos. Algunas de las vulnerabilidades detectadas en los servicios RPC se listan a continuación.

- Rpc.statd. Demonio de estado RPC NFS, componente de la arquitectura Network File System (NFS). Es parte del paquete de utilidades NFS distribuido en Linux y es empleado para comunicar información del estado a otros servicios o hosts, pero presenta también varias debilidades asociadas. Dentro de las vulnerabilidades encontradas se tiene la del formato string en el llamado a la función a la función syslog(), en la que un usuario remoto malicioso puede ejecutar código como root. Otra debilidad puede ser explotada por un atacante para crear o modificar archivos con privilegios de root. La versión de statd contenida en muchas implementaciones de UNIX contiene una condición buffer overflow. El atacante que intente explotar satisfactoriamente esta vulnerabilidad podrá ganar privilegios de root sobre el host objetivo. Una posible solución para corregir estos problemas es actualizar la versión actual de statd..
- FAM. Algunas versiones de este servicio son vulnerables, corren arbitrariamente comandos como root.
- Valid. Un atacante puede usar este servicio para hacer spoofing a mensajes de consola.

- **Cómo se ejecutará el proceso:** Para mejorar la seguridad de los servicios RPC es preciso tener en cuenta medidas como:

- Comprobar que la versión de rpc.statd no es vulnerable, para esto puede consultar a AusCERT ESB: ftp://ftp.auscert.org.au/pub/auscert/ESB/ESB-2000.222

- Filtrar el puerto tcp 111 en el router para inhabilitar o impedir el acceso a los servicios RPC desde el exterior de su red.
- Suspender el servicio portmap a menos que sea necesario. Una máquina que no usa los servicios sunrpc (por ejemplo: NFS o NIS) no necesita portmap.
- Bloquear cualquier servicio no requerido que se inicie cuando portmapper sea ejecutado, para conseguirlo puede usar el siguiente comando, el cual varía de acuerdo a la versión de Unix: /usr/bin/rpcinfo –p.
- Reemplace portmapper/rpcbind por una versión más segura tal como portmapper de Wietse Venema, ya que mejora la seguridad a través de listas de control de acceso. Es posible obtener la versión correspondiente a su sistema desde: ftp.win.tue.nl/pub/security/portmap.shar o también desde ftp://ftp.porcupine.org/pub/security/

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilitar el servicio RPC (SUN Remote Procedure Call) puerto UDP 111.
- **Lo que no se espera que suceda:** Que el servicio RPC (SUN Remote Procedure Call) puerto UDP 111 continúe activo.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar el servicio.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar el servicio este no responda.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: SNMP (Simple Network Management Protocol) puerto UDP 161

Observaciones: Evita – amenaza19.

Servicios Disponibles en el Servidor Pelícano: SNMP (Simple Network Management Protocol) puerto UDP 161

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** Estos mensajes cuidadosamente construidos por el SNMP pueden ser de gran valor para los atacantes porque pueden conocer la estructura interna de la red, efectuar un ataque de negación de servicio o cambiar la configuración de la red, situación que pretende controlar este procedimiento.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente al servicio SNMP (Simple Network Management Protocol) puerto UDP 161, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Restringir el servicio SNMP (Simple Network Management Protocol) puerto UDP 161.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicio SNMP (Simple Network Management Protocol) puerto UDP 161.

Definición del proceso

- **Introducción al proceso:** El protocolo SNMP se diseñó para permitir la administración remota de los dispositivos sobre la red, por lo tanto permite a los administradores de sistemas y de redes supervisar y configurar remotamente dispositivos sobre la red (switches y routers, entre otros). Para el protocolo SNMP la red está compuesta por un grupo de elementos básicos: Administradores o gestores ubicados en el/los equipo/s de gestión de red y; Agentes, elementos pasivos ubicados en los nodos (host, routers, modems, multiplexores, etc.) a ser gestionados, siendo estos últimos los que envían información a los primeros, relacionada con los elementos gestionados, por iniciativa propia o al ser interrogados (polling) de manera secuencial, soportada en los parámetros contenidos en sus MIB (Management Information Base).

- **Descripción de lo qué el proceso hace:** El protocolo SNMP muestra dos tipos de mensajes de administración:

  - Mensajes para cambiar el estado de un dispositivo en la red.
  - Mensajes que supervisan el estado actual de la red.

Estos mensajes cuidadosamente construidos por el SNMP pueden ser de gran valor para los atacantes porque pueden conocer la estructura interna de la red, efectuar un ataque de negación de servicio o cambiar la configuración de la red. Aunque algunos sistemas SNMP incluyen mejoras de seguridad basadas en contraseñas, para lo cual emplean el nombre de la comunidad como un password, el cual es transmitido en texto claro permitiendo que el nombre de la comunidad quede expuesto.
Cada administrador de la red debe sopesar el valor de cada servicio particular del SNMP contra el riesgo que supone el protocolo.

- **Cómo se ejecutará el proceso:** Las medidas de contención encaminadas a disminuir el impacto de las vulnerabilidades presentes en el protocolo pueden ser:

- La aplicación de los parches publicados por los diferentes proveedores de equipos y de software. Estos se pueden consultar en el sitio http://www.cert.org, en la sección “Vulnerabilities, incidents & fixes”. Allí se alertan a los usuarios sobre amenazas potenciales a la seguridad de los diferentes sistemas y se proporciona información sobre cómo evitar, minimizar o recuperarse de ataques.
- Inhabilitar el servicio SNMP si no se requiere.
- Bloquear el acceso a los puertos UDP y TCP 161 y 162, con el fin de evitar que atacantes fuera de su red local afecten dispositivos vulnerables.

```
Snmp 161/udp    #Simple Network Management Protocol (SNMP)
Snmp 162/udp    #SNMP system management messages
```

Los servicios que a continuación se detallan son menos comunes, pero

pueden ser vulnerables:

```
Snmp 161/tcp     #Simple Network Management Protocol (SNMP)
Snmp 162/tcp     #SNMP system management messages
Smux 199/tcp     #SNMP Unix Multiplexer
Smux 199/udp    #SNMP Unix Multiplexer
Synoptics-relay  391/tcp    # SynOptics SNMP Relay Port
Synoptics-relay  391/udp    # SynOptics SNMP Relay Port
Agentx            705/tcp     # AgentX
Snmp-tcp-port    1993/tcp   # cisco SNMP TCP port
Snmp-tcp-port    1993/udp  # cisco SNMP TCP port
```

Se puede bloquear también el acceso a los siguientes servicios RPC relativos a SNMP:

```
Snmp  100122   na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-utk
Snmp  100138   na.snmpv2    #SNM Versión 2.2.2
SnmpXdmid 100249
```

Filtrar la salida de tráfico hacia Internet por lo puertos anteriormente enumerados, evita que su red sea utilizada como fuente para ataques contra otros sitios.

- Filtrar el tráfico SNMP desde hosts internos no autorizados, ya que en muchas redes, sólo un número limitado de sistemas de administración de red o gestores necesitan originar peticiones SNMP, esto se logra configurando los dispositivos agentes SNMP para inhabilitar mensajes de petición provenientes de sistemas no autorizado, esta medida puede reducir, más no eliminar por completo el riesgo de ataques internos. Además puede tener efectos perjudiciales en el funcionamiento de la red debido al incremento de la carga impuesto por la filtración, por lo tanto se requiere tener gran cuidado al considerar la implementación de esta medida.
- Configurar la comunidad por defecto “public” con un nombre diferente, ya que la mayoría de los productos SNMP vienen configurados con la comunidad “public” por defecto para acceso de sólo lectura y “private” para acceso de lectura-escritura, por lo tanto se recomienda que los administradores de red cambien esos nombres de comunidad por unos de su propia elección, preferiblemente de tipo password. Sin embargo, se debe tener en cuenta que a pesar que los nombres por defecto de la comunidad sean cambiados, estos son transmitidos en texto claro y están sujetos a ataques de tipo sniffing. Por lo tanto considere SNMPv3 ya que ofrece capacidades adicionales para asegurar autenticación y privacidad como se describe en RFC2574.
- Dividir el tráfico SNMP sobre la red, especialmente en situaciones donde bloquear o inhabilitar SNMP no sea posible, ya que se puede limitar los accesos SNMP a redes aisladas que no sean de acceso público, tales como las virtual LANs (VLANs) que ayudan a segregar tráfico sobre la misma red física. Las VLANs no son infalibles ante un atacante, pero pueden hacer más difícil de

iniciar el ataque. Estos tipos de soluciones podrían requerir grandes cambios en el diseño actual de la red.

- Compartir herramientas, técnicas y experiencias. El mundo de las vulnerabilidades de los sistemas y de las redes es muy complejo, motivo por el cual se hace necesario apoyarse en organismos como CERT/CC que ofrecen foros en donde los administradores de sistemas y redes comparten ideas, técnicas y experiencias que pueden ayudar para desarrollar medidas propias de defensa. CERT/CC dispone de una lista de correo en la cual los usuarios se pueden suscribir enviando un e-mail a la dirección majordomo@cert.org. En el cuerpo del mensaje, se debe escribir: subscribe snmp-forum, y continuar con el proceso de inscripción.

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilitar el servicio SNMP (Simple Network Management Protocol) puerto UDP 161.
- **Lo que no se espera que suceda:** Que el servicio SNMP (Simple Network Management Protocol) puerto UDP 161 continúe activo.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar el servicio.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar el servicio este no responda.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar el servicio disponible en el servidor Pelícano: Syslog Puerto UDP 514

Observaciones: Evita – amenaza20.

Servicios Disponibles en el Servidor Pelícano: Syslog Puerto UDP 514

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-2-2.2, G-1-1.1.1, H-1-1.2.7
- **Cuál es el objetivo del procedimiento:** Syslog, por defecto, puede

aceptar mensajes de log de hosts arbitrariamente enviados al puerto local UDP del syslog. Esta situación abre la posibilidad de un ataque de negación de servicio, en caso de que el puerto se inunde con mensajes más rápidos de los que el demonio del syslog pueda procesar, también mensajes fraudulentos pueden ser enviados deliberadamente al puerto, con el objetivo de obtener privilegios en el sistema y llegar a ejecutar código como root, hacia el control de estas vulnerabilidades se orienta este procedimiento.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano, en especial y más exactamente al servicio Syslog Puerto UDP 514, extensible a los demás servidores críticos de la universidad.
- **Qué función se espera que este proceso ejecute**: Restringir el servicio Syslog Puerto UDP 514.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros, servicio Syslog Puerto UDP 514.

Definición del proceso

- **Introducción al proceso:** El demonio syslog (Syslog Daemon) se activa automáticamente al arrancar el sistema Unix, se encarga de guardar informes sobre el funcionamiento de la máquina, además recibe mensajes de las diferentes partes del sistema (núcleo, programas, dispositivos) y los envía y/o almacena en diferentes localizaciones, tanto locales como remotas, acorde a criterios definidos en el fichero de configuración /etc/syslog.conf, el cual especifica las reglas a seguir para gestionar el almacenamiento de los mensajes del sistema
- **Descripción de lo qué el proceso hace:** Syslog puede recibir mensajes de log desde tres fuentes y estas son:

- /dev/klog: dispositivo especial, usado para leer mensajes generados por el kernel.
- /dev/log: Unix domain socket, usado para leer mensajes generados por procesos corriendo sobre la máquina local.
- UDP puerto 514: Internet domain socket, usado para leer mensajes generados sobre la red de área local desde otras máquinas.
- Syslog, por defecto, puede aceptar mensajes de log de hosts arbitrariamente enviados al puerto local del UDP del syslog. Esta situación abre la posibilidad de un ataque de negación de servicio, en caso de que el puerto se inunde con mensajes más rápidos de los que el demonio del syslog pueda procesar, también mensajes fraudulentos pueden ser enviados deliberadamente al puerto, con el objetivo de obtener privilegios en el sistema y llegar a ejecutar código como root.

- **Cómo se ejecutará el proceso:** Estas consideraciones deben ser tenidas en cuenta para un mejor aprovechamiento del recurso de auditoría brindado por la utilidad syslog:

- Asegurar un suficiente espacio en el disco para poder almacenar los mensajes de log deseables. Dicho espacio requerido dependerá de la configuración y la utilización del sistema de discos. Se debe revisar el tamaño de los archivos de log después de establecer la configuración inicial y después de realizar cambios en la misma. Se recomienda controlar manualmente el tamaño de los archivos de log sobre un periodo de tiempo de modo que se pueda ajustar de acuerdo a las necesidades.

- Estar alerta ante posibles ataques de negación del servicio, ya que un atacante puede crear mensajes con el objetivo de consumir todo el espacio disponible en disco, provocando con esto que cuando se llene, no se puedan almacenar mensajes log nuevos, trayendo como consecuencia además, que se pierda el patrón del ataque del intruso así como también los mensajes críticos, por lo tanto como medida de protección los archivos syslog deben ser almacenados en una partición diferente para evitar que se confundan o solapen con estos servicios (servidores e-mail, directorios del spool para impresoras). Otro ataque de negación del servicio puede presentarse cuando la carga de procesamiento en un sistema que genera mensajes de log es alta, produciendo que el sistema no pueda almacenar o remitir mensajes de log a un loghost, por

lo tanto se debe considerar la carga tanto para los sistemas que generan mensajes de log como para los sistemas que sirven como loghosts., además de disminuir la colocación de otros servicios en los servidores que funcionan como loghosts.

- La no existencia de autenticación de mensajes de log, hace que el acceso al proceso syslog deba prohibirse a usuarios externos a la red como medida de protección en contra de mensajes maliciosos creados por ellos. Lo anterior se logra filtrando los paquetes en la interfaz entre cualquier red pública (por ejemplo, Internet) y la red de área local. Tampoco es necesario aceptar mensajes syslog externos a la red interna, y se debe aplicar el filtro a toda dirección de destino interna.

- Tenga en cuenta que los usuarios locales por lo general tienen la capacidad de crear mensajes arbitrarios de log usando utilidades como logger, amenaza para la cual no hay protección

- Identificar nuevos mensajes syslog. Lo anterior debido a que cada aplicación origina mensajes diferentes en diversos formatos al usar syslog. Esto hace difícil conocer todos los mensajes posibles (su formato, prioridad y fuente), por lo tanto se recomienda almacenar cada mensaje de log producido por una aplicación dada, para posteriormente revisar los resultados con el fin de lograr familiarizarse con las salidas, luego de este proceso es posible identificar los mensajes más significativos para detectar señales de intrusión mediante del uso de la documentación del programa, manuales o el código fuente (si se encuentra disponible).

- **Cuándo se ejecutará el proceso**: Especialmente al iniciar el montaje y configuración del servidor Web.
- **Lo que se espera que suceda durante la ejecución del proceso:** Inhabilitar el servicio Syslog Puerto UDP 514.
- **Lo que no se espera que suceda:** Que el servicio Syslog Puerto UDP 514 continúe activo.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Volver a intentar cerrar el servicio.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al ejecutar el servicio este no responda.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos	
• **Qué se hará si se presenta un problema en el proceso:** Repetir la operación anteriormente descrita.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Protección contra la amenaza que puede ocasionar la Identificación de direcciones IP - Servidores UIS. **Observaciones: Evita – amenaza21.** Identificación de direcciones IP - Servidores UIS.
Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C
Propósito del procedimiento: • **Qué estándar cumple:** D-2-2.6, D-2-2.7, G-1-1.1.3 • **Cuál es el objetivo del procedimiento:** Evitar que la exploración de puertos le permita a un atacante obtener listas de direcciones IP, que lo conduzcan a conocer información importante como nombres de servidores DNS y de correo, de empleados, números telefónicos entre otros.
Alcance del procedimiento • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Servidor Pelícano y demás servidores críticos UIS. • **Qué función se espera que este proceso ejecute**: Restringir la exploración de puertos con el fin de evitar que un atacante pueda obtener listas de direcciones IP, nombres de servidores DNS y de correo, de empleados, números telefónicos entre otros. • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de servidores Web seguros.

Definición del proceso

- **Introducción al proceso:** Explorar puertos es equivalente a un ladrón que palpa las paredes en la búsqueda de puertas y ventanas para poder cometer su ilícito, es decir palpar que sistemas se encuentran activos y cuáles son accesibles a través de Internet, mediante el uso de una variedad de técnicas y herramientas de búsqueda automatizadas, por lo tanto este procedimiento pretenden minimizar o controlar estos riesgos.
- **Descripción de lo qué el proceso hace:** Realizar un seguimiento de las actividades de exploración de puertos para identificar al atacante, con el objeto de localizarlo, obtener pruebas y depende de las políticas tomar represalias.

- **Cómo se ejecutará el proceso:** Los atacantes suelen utilizar la exploración de puertos para determinar qué puertos UDP y TCP están a la escucha en los sistemas remotos. Detectar una actividad de exploración de puertos es de gran importancia para advertir cuándo se puede producir un ataque y quién lo va a llevar a cabo. Los principales métodos de exploración de puertos consisten en programas IDS (Sistemas detección de intrusos) que se encargan de realizar un análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones. Son recomendables porque proporcionan conocimiento del entorno de ataque, alertan ante actividades sospechosas y adicionalmente brinda un registro adicional de evidencias que pueden servir como evidencia judicial. Los IDS no son suficientes, debido a que estos sólo detectan ataques conocidos, por lo tanto es posible y algunas veces engañarlos, por lo tanto es conveniente dejar la defensa pasiva y pensar en defensas o respuesta activas o automáticas, que son todas aquellas acciones que se ejecutan sin intervención humana al detectar un ataque. Por lo tanto interesa responder ante un ataque, transformando el esquema de IDS en un elemento activo. Dentro de los tipos de respuesta automática tenemos: la respuesta automática y la manual, superando la automática a la manual por rapidez, escalabilidad, registro, integración y precio. Dentro de las respuestas automáticas tenemos:

- Registro: tiene como características la activación de registros adicionales, todavía un mecanismo pasivo, útil para monitorización, como por ejemplo la activación del sistema de auditoría de Unix ante un acceso sospechoso a **/etc/passwd.**
- Bloqueo: suprime interacciones entre atacante y atacado siendo el esquema más habitual, es un mecanismo activo, por ejemplo: bloqueo en cortafuegos intermedio, suspensión de trabajos en un host.
- Ataque: las acciones son agresivas contra el intruso, también es un mecanismos activo, se tendrá que valorar por el Comité de Seguridad Informática si es ética esta respuesta. Ejemplo: lanzamiento de un ataque de negación de servicio contra el intruso.
- Recuperación: detectan el cambio de estado de un recurso atacado y lo devuelven a su estado anterior, es un mecanismo activo. Por ejemplo un sistema que restaura el contenido de una página web si detecta una modificación. En muchas ocasiones difíciles de implantar, por ejemplo actualización frecuente de páginas web.

- Decepción: se encargan de dejar aburrido o decepcionado al atacante, es un mecanismo activo, la pregunta que podría hacerse es: ¿Si sirve de algo la decepción al atacante?. Como ejemplo se puede dar la detección de un intruso intentando hacer una maniobra ilegal, en la que le aparece un mensaje "Sonría a la cámara oculta".

Dentro de los IDS más recomendados se tienen los siguientes:

- Snort: herramienta localizable en http://www.snort.org/, es sistema experto en tiempo real, abierto, incorpora muchas herramientas dentro de ellas la respuesta automática ante intrusiones.
- TripWire: localizable en http://www.tripwire.com/, es un verificador de integridad basado en máquina, no incorpora respuestas automática ante intrusiones, pero es fácil integrarla en el sistema
- PHF: proporciona información falsa (pero creíble) al atacante, mientras registra sus actividades, dentro de sus características incorpora un fichero único en PERL efectivo, fácil de instalar y gestionar.

También el firewall posee mecanismos (algunos combinan funciones con IDS) para filtrar la exploración de puertos y consisten en implantar y mejorar los filtros o reglas implantadas.

- **Cuándo se ejecutará el proceso**: El proceso debe actuar permanentemente.
- **Lo que se espera que suceda durante la ejecución del proceso:** Que tanto los IDS como el Firewall detecten exploraciones de puertos.
- **Lo que no se espera que suceda:** Que los intrusos logren efectuar su maniobra de ataque y no sean detectados.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Revisar o actualizar las versiones del IDS, como también la revisión de las reglas implantadas en el firewall.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas de intrusión estas sean reportadas por los mecanismos IDS o Firewall.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar tanto el Administrador Central de Seguridad Informática que tiene bajo su responsabilidad el manejo y supervisón de tecnologías de seguridad como también el administrador de Usuarios y Accesos encargado de organizar los usuarios y sus respectivos accesos, quien enviarán un reporte-informe de inconvenientes de seguridad semanal o como estime conveniente el Director de Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática.
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Revisar las reglas o filtros del IDS o Firewall.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Protección contra la amenaza que puede ocasionar la Exploración de puertos al Firewall de la UIS y routers CISCO ETB y TELECOM.
Observaciones: Evita – amenaza22.
Debilidades encontradas en el Firewall de la UIS (amenazas provenientes externamente):
Exploración de puertos al Firewall de la UIS y routers CISCO ETB y TELECOM.

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** D-2-2.6, D-2-2.7, G-1-1.1.3, G-1-1.2.1, G-1-1.3.1
- **Cuál es el objetivo del procedimiento:** Casi todos lo cortafuegos o firewall emiten un rastro electrónico único, o sea, con una sencilla exploración de puertos, de captura de mensajes, los atacantes pueden determinar con efectividad el tipo, versión y reglas de casi todos los cortafuegos instalados en la red. ¿Por qué resulta importante esta identificación?. Porque una vez que se conocen los cortafuegos, pueden comenzar la búsqueda de debilidades e intentar explotarlas, igualmente ocurre con otros dispositivos de red, por lo tanto este procedimiento intenta minimizar la posibilidad de ataque a estos dispositivos.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Firewall de la UIS y routers CISCO ETB y TELECOM, extensible a los demás dispositivos de red variando de acuerdo a las marcas.
- **Qué función se espera que este proceso ejecute**: Restringir mediante filtros y puesta a punto de firmas de detección la exploración de puertos en el Firewall de la UIS y routers CISCO ETB y TELECOM.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás dones, además de montaje y configuración de Firewall y dispositivos routers CISCO seguros o demás marcas.

Definición del proceso

- **Introducción al proceso:** Los cortafuegos o firewalls son dispositivos diseñados para proteger el tráfico entrante y saliente de una organización. Por lo tanto es muy importante la configuración del mismo para evitar la penetración especialmente externa de un intruso.
- **Descripción de lo qué el proceso hace:** Realizar un seguimiento de las actividades de exploración de puertos para identificar el atacante, con el objeto de localizarlo, obtener pruebas o tomar represalias, revisando además el filtrado de los diferentes puertos para evitar la intromisión de un atacante.

- **Cómo se ejecutará el proceso:** Los atacantes suelen utilizar la exploración de puertos para determinar qué puertos están a la escucha en los sistemas remotos. Detectar una actividad de exploración de puertos es de gran importancia para advertir cuándo se puede producir un ataque y quién lo va a llevar a cabo. Los principales métodos contra la exploración de puertos consisten en Cortafuegos y programas IDS (Sistemas detección de intrusos) que se encargan de realizar un análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones. Son recomendables porque proporcionan conocimiento del entorno de ataque, alerta ante actividades sospechosas y adicionalmente brinda un registro adicional de evidencias que pueden servir como evidencia judicial. Los IDS no son suficientes, debido a que estos sólo detectan ataques conocidos, por lo tanto es posible y algunas veces engañarlos, por lo tanto es conveniente dejar la defensa pasiva y pensar en defensas o respuesta activas o automáticas, que son todas aquellas acciones que se ejecutan sin intervención humana al detectar un ataque. Por lo tanto interesa responder ante un ataque, transformando el esquema de IDS en un elemento activo. Dentro de los tipos de respuesta automática tenemos la respuesta automática y la manual, superando la automática a la manual por rapidez, escalabilidad, registro, integración, precio. Dentro de las respuestas automáticas tenemos:

- Registro: tiene como características la activación de registros adicionales, todavía un mecanismo pasivo, útil para monitorización, como por ejemplo la activación del sistema de auditoría de Unix ante un acceso sospechoso a **/etc/passwd.**
- Bloqueo: suprime interacciones entre atacante y atacado siendo el esquema más habitual, es un mecanismo activo, por ejemplo: bloqueo en cortafuegos intermedio, suspensión de trabajos en un host.
- Ataque: las acciones son agresivas contra el intruso, también es un mecanismos activo, se tendrá que valorar por el Comité de Seguridad Informática si es ética esta respuesta. Ejemplo: lanzamiento de un ataque de negación de servicio contra el intruso.
- Recuperación: detectan el cambio de estado de un recurso atacado y lo devuelven a su estado anterior, es un mecanismos activo. Ejemplo: sistema que restaura el contenido de una página web si detecta una modificación. En muchas ocasiones difíciles de implantar (por ejemplo actualización frecuente de páginas web.
- Decepción: se encargan de dejar aburrido o decepcionado al atacante, es

un mecanismo activo, la pregunta que podría hacerse es si sirve de algo la decepción al atacante?. Por ejemplo se detecta a un intruso intentando hacer una maniobra ilegal, en la que le aparece un mensaje “Sonría a la cámara oculta”.
Dentro de los IDS más recomendados se tienen los siguientes:

- Snort: herramienta localizable en http://www.snort.org/, es sistema experto en tiempo real, abierto, incorpora muchas herramientas dentro de ellas la respuesta automática ante intrusiones.
- TripWire: localizable en http://www.tripwire.com/, es un verificador de integridad basado en máquina, no incorpora respuestas automática ante intrusiones, pero es fácil integrarla en el sistema
- PHF: proporciona información falsa (pero creíble) al atacante, mientras registra sus actividades, dentro de sus características incorpora un fichero único en PERL efectivo, fácil de instalar y gestionar.

También el firewall posee mecanismos o algunos combinan funciones con IDS, por lo tanto es conveniente estar revisando los filtros o reglas implantadas.

- **Cuándo se ejecutará el proceso**: En forma permanente.
- **Lo que se espera que suceda durante la ejecución del proceso:** Que filtros del firewall detecten y eviten exploraciones de puertos y por ende las posibles intrusiones.
- **Lo que no se espera que suceda:** Que los intrusos logren efectuar su maniobra de ataque y penetren nuestra organización desde afuera.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Revisar o actualizar los filtros o reglas firewall.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas de intrusión externas estas sean reportadas por los mecanismos IDS o firewall.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar tanto el Administrador Central de Seguridad Informática que tiene bajo su responsabilidad el manejo y supervisón de tecnologías de seguridad como también el administrador de Usuarios y Accesos encargado de organizar los usuarios y sus respectivos accesos quien enviarán un reporte-informe de inconvenientes de seguridad semanal o como estime conveniente el Director de Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática.
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos
Qué se hará si se presenta un problema en el proceso: Revisar las reglas o filtros del IDS o Firewall.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar la violación al WEBSENSE (mecanismo que administra, controla y optimiza el uso de ancho de banda de acceso a Internet.

Observaciones: Evita – amenaza23.

Violación al WEBSENSE (mecanismo que administra, controla y optimiza el uso de ancho de banda de acceso a Internet).

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** G-2-2.1.2, G-2-2.2.4, G-2-2.2.5, G-2-2.2.6, G-2-2.4.5, G-2-2.4.6, G-2-2.4.7
- **Cuál es el objetivo del procedimiento:** La UIS posee y paga derechos por usar un software para el control de contenidos de la web denominado WEBSENSE, con el objetivo de evitar que tanto sus empleados como los estudiantes puedan acceder a páginas de ocio y entretenimiento en tiempos laborales y de estudio, este procedimiento pretende evitar que se siga violando el software de control de contenidos Websense.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Al software control de contenidos Websense, servidores web.
- **Qué función se espera que este proceso ejecute**: Restringir mediante filtros el acceso de estudiantes y trabajadores a páginas de ocio y entretenimiento en tiempos laborales y de estudio.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de Firewall , además del control de contenidos Websense.

Definición del proceso

- **Introducción al proceso:** El control de contenidos de la web denominado WEBSENSE, debe evitar que tanto sus empleados como los estudiantes puedan acceder a páginas de ocio y entretenimiento en tiempos laborales y de estudio, pero es violado a menudo por estudiantes de la UIS.

- **Descripción de lo qué el proceso hace:** Filtrar las diferentes páginas de ocio y entretenimiento para que el estudiante y empleado no puede acceder en horas de estuido o laborales de acuerdo a horarios establecidos por las directivas de la Universidad.

- **Cómo se ejecutará el proceso:** El software de Websebse se adapta para brindar apoyo a la política de acceso a Internet a la UIS. Websense puede acomodarse muy bien a cualquier política de acceso a Internet, ya que cuenta con ocho opciones de administración diferentes y flexibles. Además de poder bloquear y permitir acceso, otras características que se incluyen son:

- Cuotas basadas en tiempo: Con cuotas basadas en tiempo, se puede permitir que los empleados tengan acceso a páginas no relacionadas con el trabajo por períodos de tiempo limitados, pero apropiados. Por ejemplo, permitir el acceso a sitios para operaciones bancarias o compras por hasta 20 minutos por día.
- Continuar y/o diferir: Permita que los usuarios escojan "continuar" navegando en las páginas bloqueadas que ellos consideren relacionadas con el trabajo o "diferir" la navegación personal a otro tiempo fuera del horario de trabajo. Las páginas diferidas están automáticamente marcadas para los empleados en AfterWork.com, (Después del Trabajo.com), que es una página gratuita, hospedada y mantenida por Websense.
- Horas del día: Todas las opciones de filtración pueden establecerse por horas específicas del día. Por ejemplo, se puede bloquear el acceso a compras durante las horas laborables y permitir el acceso en todas las demás horas.
- Políticas de acceso a Internet a la medida: Se puede establecer el acceso a Internet por usuario, grupo, departamento, estación de trabajo o red.
- Listas con "Sí": Para permitir el acceso únicamente a sitios específicos.
- La base de datos más completa y exacta en la industria: Más de más de 3,3 millones de sitios, que representan más de 600 millones de páginas Web, organizadas en 75 o más categorías, proporciona una filtración de Internet completa, precisa y detallada.
- Filtro por nombre y tipo de archivo: Reglamente las descargas de archivos por nombre o extensión de archivo, incluyendo audio, video e imágenes de anuncios. Ponga límites para bajar jpegs de MP3s y otros archivos intensivos de amplitud de banda en su red.
- Categorías dinámicas de base de datos: Reciba automáticamente nuevas categorías de base de datos de Websense, conforme vayan surgiendo nuevos tópicos en Internet.
- Filtración opcional de palabras clave en URLs: Incremente la filtración mediante el bloqueo de sitios cuyos URLs contengan palabras específicas, tales como "sexo" y "porno".
- Reporte sobre la actividad en Internet: Elija entre más de 60 reportes,

tablas y gráficas, incluyendo los sitios visitados más frecuentemente, así como los usuarios más activos.

- Programación y entrega de reportes: Programe los reportes para que sean producidos diaria, semanal o mensualmente y entréguelos automáticamente vía correo electrónico.
- Páginas de bloqueo hechas a la medida: Confeccione, a la medida de sus necesidades, la página que los usuarios verán cuando hayan tenido acceso a un sitio bloqueado. Cree su propia página con el logotipo y la política de acceso a Internet de su compañía, edite texto en la página de Websense o utilice la página por omisión de Websense.
- Actualizaciones automáticas diarias: Las actualizaciones a la base de datos son bajadas automáticamente a su servidor todos los días para garantizar que usted esté utilizando la base de datos más nueva y más confiable posible. Se bajan únicamente cambios y adiciones, para ahorrarle amplitud de banda y tiempo.
- Alerta administrativa: Reciba notificación por correo electrónico de eventos importantes del sistema Websense.
- Aviso de duración de la política de acceso: Cuando los usuarios solicitan sitios que han sido bloqueados, hágales saber si el acceso a estos sitios es permitido y cuándo.
- Requisitos para Cisco PIX: Cisco PIX Firewall serie 500 con 16 MB de RAM, 2 MB de Flash, PIX firmware 4.4 o superior.

Por lo tanto se debe estar actualizando permanentemente los filtros de las páginas a filtrar para evitar las violaciones a estos sistemas.

- **Cuándo se ejecutará el proceso**: En forma permanente.
- **Lo que se espera que suceda durante la ejecución del proceso:** Que los estudiantes y personal de la UIS no puedan violar el Websense.
- **Lo que no se espera que suceda:** Que los estudiantes accedan a páginas filtradas.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Revisar o actualizar los filtros.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas no se puedan acceder a páginas filtradas.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Contrato con Websense.

Problemas de los procesos	
• **Qué se hará si se presenta un problema en el proceso:** Revisar las reglas o filtros del IDS, Firewall y websense.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:
Protección contra la amenaza que puede ocasionar la violación de los servidores de correo de la UIS (Cóndor y Albatros). **Observaciones: Evita – amenaza24.** Violación de los servidores de correo de la UIS (Cóndor y Albatros).
Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C
Propósito del procedimiento: • **Qué estándar cumple:** G-2-2.4.4, G-2-2.4.6, G-2-2.4.7, G-2-2.4.10 • **Cuál es el objetivo del procedimiento:** En la UIS como en cualquier organización o persona tiene derecho a su privacidad y mucho más a la información transmitida mediante correo electrónico y aún más de sus docentes, se encontró que mediante algunos software como FileZilla_2_2_7a_setup, que es un programa para manejar archivos mediante ftp, al efectuarse la conexión a Cóndor mediante su respectiva IP como un usuario válido, se observó que perfectamente se podía acceder a otras carpetas privadas de docentes de la UIS y leer su información o archivos personales sin ningún inconveniente, el control de esta debilidad es el objetivo de este procedimiento.
Alcance del procedimiento • **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** A servidores de correo de la UIS, como por ejemplo Cóndor y Albatros. • **Qué función se espera que este proceso ejecute**: Evitar que intrusos puedan acceder a archivos privados de docentes y personal de la universidad empleando software para manejar archivos mediante FTP. . • **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de Servidores Web , protocolo FTP.

Definición del proceso

- **Introducción al proceso:** FileZilla_2_2_7a_setup, que es un programa para manejar archivos mediante ftp, al efectuarse la conexión a Cóndor mediante su respectiva IP como un usuario válido, se observó que perfectamente se podía acceder a otras carpetas privadas de docentes de la UIS, por lo tanto es necesario evaluar la necesidad de ejecutar un servidor FTP, por lo tanto se deben aplicar últimos parches de seguridad desarrollados y eliminar o reducir el número de directorios de escritura universal disponibles.

- **Descripción de lo qué el proceso hace:** Muchos servidores FTP permiten accesos anónimos, permitiendo a cualquier usuario iniciar una sesión en un servidor FTP sin necesidad de autenticación. Normalmente el sistema de archivos al que se permite el acceso se limita a una rama particular del árbol de directorios. Sin embargo en otras ocasiones, el servicio FTP anónimo permitirá al usuario moverse por la estructura completa del directorio, para contrarrestar la situación es posible
- **Cómo se ejecutará el proceso:** FTP, o File Transfer Protocol (Protocolo de Transferencia de Archivos), es uno de los protocolos más comunes utilizados actualmente. Le permite cargar y descargar archivos desde/hacia sistemas remotos. A veces se utiliza FTP para obtener acceso a sistemas remotos o para almacenar archivos ilegales. Muchos servidores FTP permiten accesos anónimos, permitiendo a cualquier usuario iniciar una sesión en un servidor FTP sin necesidad de autenticación. Normalmente el sistema de archivos al que se permite el acceso se limita a una rama particular del árbol de directorios. Sin embargo en otras ocasiones, el servicio FTP anónimo permitirá al usuario moverse por la estructura completa del directorio. Así los atacantes pueden moverse a sus anchas por los archivos de otros usuarios y lo que es más peligroso obtener archivos de configuración tales como **/etc-passwd** . Para complicar la situación, muchos servidores FTP disponen de directorios en los que puede escribir cualquiera. Uno de estos directorios en combinación con un acceso de tipo anónimo es una garantía de que sucederá algún tipo de accidente. Los atacantes pueden colocar un archivo **.rhosts** en directorio **home** de un usuario, permitiendo a los atacantes hacer un rlogin al sistema atacado. Además muchos piratas de software abusan de los servidores FTP, almacenando software de inicio legal en directorios ocultos. Si la utilización de su red se triplica en un día, podría ser una clara indicación de que sus sistemas están siendo utilizados para propósitos no demasiado claros.
Aunque FTP es muy útil, permitir acceso anónimo a FTP puede resultar peligroso para la salud del servidor. Evalúe la necesidad de ejecutar un servidor FTP y decida si tiene que permitir el acceso anónimo a su servicio FTP. Muchos sitios tienen que permitir acceso anónimo vía FTP, sin embargo deben ponerse todos los medios necesarios para garantizar la seguridad del servidor. Asegúrese de que está aplicando los últimos parches de seguridad desarrollados y elimine o reduzca el número de directorios de escritura universal disponibles.
  - **Cuándo se ejecutará el proceso**: Al configurar el servicio FTP.
  - **Lo que se espera que suceda durante la ejecución del proceso:** Que los atacantes no puedan desplazarse por las diferentes carpetas y archivos

tanto de profesores como de personal de la UIS.

- **Lo que no se espera que suceda:** Que el atacante acceda las carpetas y archivos de docentes y empleados de la UIS mediante el protocolo FTP.
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Revisar o actualizar los parches y medidas.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas no se puedan acceder a carpetas y ficheros de docentes y empleados UIS.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

Qué se hará si se presenta un problema en el proceso: Revisar las consideraciones y parches acerca del protocolo FTP.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar la alteración malintencionada del software de aplicación, mediante la inclusión dentro del código de programas que se instalan como: virus, caballos de Troya u otras amenazas. Exploits de vulnerabilidades conocidas en programas y servicios

Observaciones: Evita – amenaza25.

Alteración malintencionada del software de aplicación, mediante la inclusión dentro del código de programas que se instalan como: virus, caballos de Troya u otras amenazas.
Exploits de vulnerabilidades conocidas en programas y servicios.

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-1-1.4, B-1-1.5, B-4-4.1, B-4-4-2, H-3-3.1, H-3-3.2
- **Cuál es el objetivo del procedimiento:** Los fallos y errores de diseño no sólo en las aplicaciones sino también en los núcleos de los sistemas operativos son fuentes de amenazas a la seguridad de todo sistema informático, por tanto los errores o bugs en el código fuente de las aplicaciones constituyen una de las amenazas a la seguridad que más problemas han causado a la comunidad de la seguridad informática. Generalmente estas complicaciones no se originan por falta de conocimiento en la realización de programas seguros, sino más bien en que resulta casi imposible no cometer alguna equivocación en miles de líneas de código.

Con frecuencia muchos programas son afectados por uno de los errores más comunes y utilizados por atacantes como es el desbordamiento de pila (snack smashing), también conocido como buffer overflow). A pesar de que los programas en especial los setuidados, son en la actualidad más seguros; es muy frecuente que un atacante intente acceder a un sistema consiguiendo privilegios de administrador a través de un buffer overflow.

Otra amenaza a la seguridad son los exploits, disponibles en Internet (programas que aprovechan un error en otro programa o servicio para violar la política de seguridad del sistema y ganar privilegios sobre éste), existen para casi todas las versiones de Unix e incluyen el código necesario para ejecutar shells sobre cualquier sistema operativo y arquitectura, por lo tanto las contramedidas a tomar son el objetivo de este principal de este procedimiento.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Al software de aplicación
- **Qué función se espera que este proceso ejecute**: Evitar la inclusión de virus, caballos de Troya u otras amenazas dentro del código de programas.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en sistema operativo Unix y demás clones, además de montaje y configuración de Servidores Web, protocolo FTP, software antivirus.

Definición del proceso

- **Introducción al proceso:** La instalación de software por parte del administrador del sistema debe provenir de una fuente confiable, y debe ser precavido en caso de que el programa afecte así sea en poco grado funciones delicadas del sistema operativo (las medidas de precaución pueden ser la prueba del software en una máquina de testeo, o en entornos cerrados con chroot()).
- **Descripción de lo qué el proceso hace:** Cuando se instalan nuevas aplicaciones de Unix o se actualizan las existentes, se debe tener mucho cuidado con los archivos setuidados que estas aplicaciones instalan por defecto en la máquina, ya que en algunos archivos ejecutables no se hace necesario este bit activo, motivo por el cual se debe resetear el bit de los ficheros que no lo necesiten por parte del administrador.
- **Cómo se ejecutará el proceso:** Como medidas acertadas para reducir el impacto de las vulnerabilidades en las diferentes aplicaciones figuran:

- Para disminuir el impacto que los buffer overflow pueden causar en los sistemas se necesita una estrecha colaboración entre fabricantes, administradores y programadores, ya que los primeros deben de tratar de verificar más la robustez de los programas críticos antes de sacarlos al mercado, los administradores deben procurar mantener al mínimo el número de ficheros setuidados o setgiados en sus sistemas y los programadores unir sus esfuerzos para lograr generar código con menos puntos de desbordamiento.
- Mantener actualizados frecuentemente las aplicaciones instaladas en el sistema y los parches. Por lo general los desarrolladores de software sacan al mercado nuevas versiones de sus productos con correcciones a problemas de seguridad y a errores detectados en las versiones anteriores. Estas mejoras a la seguridad comúnmente llamados parches, lo mismo que las actualizaciones liberadas se hacen generalmente vías correo electrónico. El administrador se debe suscribir a las listas de correo de su proveedor de software y sistema operativo específicos.
- Estar atento a la descarga de los parches más recientes tanto del sistema operativo como los de software específico (por ejemplo: DNS, servidor web, etc) desde el sitio del respectivo proveedor.
- Instalar cualquier parche de seguridad que todavía no haya instalado y se recomiende para su sistema, aunque se debe estar alerta ya que algunos parches pueden volver a habilitar configuraciones por defecto, por tal motivo, es importante informarse tanto de las características como debilidades del parche o el paquete software que se va a instalar, dicha información se puede obtener en el sitio desde el cual realizará la descarga o en sitios dedicados a la seguridad informática como por ejemplo www.cert.org.
- Comprobar la firma digital de cualquier archivo firmado. Para lo cual se puede auxiliar de herramientas de encripción como PGP y GnuPG, ya que pueden usarse para firmar archivos como también para verificar dichas firmas.
- De llegarse a proporcionar una suma de verificación MD5, compruebe el valor de dicha suma para estar seguro que usted ha descargado una copia válida. Algunas herramientas para verificar sumas MD5 están contenidas en varios de los sistemas operativos actuales, por ejemplo md5sum (Linux) o md5

(FreeBSD). Una implementación de MD5 está disponible vía FTP anónimo en: ftp://coast.cs.purdue.edu/pub/tools/unix/crypto/md5/.

- En caso de proporcionar una suma de verificación genérica sum(1), verifíquela cuidadosamente ya que sum(1) sólo detectará modificaciones durante la transferencia del archivo (download), más no detectará los cambios maliciosos hechos al software antes de comenzar la descarga, por este motivo es preferible verificar los archivos con MD5 o PGP/GnuPG.

Es muy importante suscribirse a listas de correo ofrecidas por sitios web dedicados a temas sobre seguridad informática como: www.hispasec.com, www.cert.org, www.isalliance.org, entre otros, con el fin de estar al tanto de problemáticas y contramedidas relacionadas con el activo y cambiante mundo de la seguridad informática. Por ejemplo Silicon Graphics, proveedor del sistema operativo IRIX instalado en Pelícano; brinda soporte a temas relacionados con seguridad informática a todos sus usuarios, en la dirección web: http://www.sgi.com/support/security/. Por otro lado, IBM proveedor del software de aplicación Informix, publica noticias de actualizaciones y parches liberados para sus productos en la dirección web:http://www.ibm.com/support/.

- **Cuándo se ejecutará el proceso**: En forma continuada y permanente.
- **Lo que se espera que suceda durante la ejecución del proceso:** Minimizar la posibilidad de alteración de programas de aplicación.
- **Lo que no se espera que suceda:** La inclusión o alteración de programas de aplicación..
- **Las acciones que se tomarán si ocurre un hecho imprevisto:** Revisar o actualizar los parches y medidas.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas no se puedan acceder a carpetas y ficheros de docentes y empleados UIS.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Revisar las consideraciones y parches acerca del protocolo FTP.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar la alteración, divulgación, modificación, interceptación, pérdida total o parcial de los datos.

Observaciones: Evita – amenaza26.

Alteración, divulgación, modificación, interceptación, pérdida total o parcial de los datos.

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** B-1-1.5, C-2-2.1.1, C-2-2.1.2, C-2-2.1.3, C-2-2.1.5, C-2-2.1.7, C-3-3.3, C-3-3.12, C-4-4.5, D-2-2.1, D-2-2.2, D-4.4.1, G-1-1.1.1, G-1-1.1.2, G-1-1.1.4, G-1-1.1.5, G-1-1.2.1, G-1-1.2.2.
- **Cuál es el objetivo del procedimiento:** La interceptación o eavesdropping, (conocida también como passive wiretapping) se puede definir como el proceso mediante el cual un agente obtiene o captura información (en claro o cifrada) que no le iba dirigida. Lo más peligroso del eavesdropping es que es muy difícil de detectar mientras que se produce, ya que este tipo de ataque se comporta en un comienzo como un ataque pasivo, es decir que el atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta, luego el mismo atacante emplea la información capturada, convirtiendo el ataque en activo. Un mecanismo de interceptación comúnmente utilizado es el sniffing. Este procedimiento pretende contrarrestar este tipo de amenaza.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Puntos críticos de la red, canales de datos, sistemas de Bases de Datos, los sistemas y servidores de la D.S.I de la UIS.
- **Qué función se espera que este proceso ejecute**: Evitar la alteración, divulgación, modificación, interceptación, pérdida total o parcial de los datos.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en encriptamiento o cifrado a nivel de hardware y software, sistemas de respaldo, backups.

Definición del proceso

- **Introducción al proceso:** La información almacenada en el sistema puede perderse o modificarse debido a varias causas como:

- Daños en los componentes hardware de la máquina.
- Borrado o modificación, accidental o intencional, de los datos almacenados en la base de datos.
- Pérdida o modificación de los programas de aplicación almacenados en los discos duros de la máquina.

- **Descripción de lo qué el proceso hace:** Ante estas problemáticas las copias de seguridad (backups) son frecuentemente el único mecanismo de recuperación que poseen los administradores para restaurar una máquina a su estado de normal funcionamiento. Por tanto, es de suma importancia una correcta política para realizar, almacenar y restaurar los backups, resultando vital en la planificación de la seguridad de todo sistema.

- **Cómo se ejecutará el proceso:** Cuando se habla de seguridad de los datos implica la protección a la información del sistema, y esta comprende no sólo la información que está almacenada en él, sino también la información que se transmite entre diferentes equipos.

Respecto a los ataques de interceptación existen diversas soluciones; dentro de las más económicas están las que usan aplicaciones software de cifrado para realizar las comunicaciones o el almacenamiento de la información. A nivel físico, no se debe descuidar las tomas de red libres, donde un intruso con un portátil puede conectarse para capturar tráfico; es recomendable analizar regularmente la red para verificar que todas las máquinas activas están autorizadas.

Otras soluciones también efectivas pero mucho más costosas contra la interceptación a nivel físico son las que utilizan dispositivos de cifra (no simples programas, sino hardware), generalmente chips que implementan algoritmos como DES. La única diferencia en muchas ocasiones de los dispositivos de cifra con respecto a las implementaciones software es la velocidad. Otra solución que se puede utilizar es el cableado en vacío para evitar la interceptación de datos que viajan por la red: la idea es situar los cables en tubos donde artificialmente se crea el vacío o se inyecta aire a presión; si un atacante intenta “pinchar” el cable para interceptar los datos, rompe el vacío o el nivel de presión y el ataque es detectado inmediatamente. Esta solución es enormemente cara y solamente se aplica en redes de perímetro reducido para entornos de alta seguridad.

El medio habitual que los administradores utilizan para restaurar un sistema que por diversas causas ha dejado de funcionar adecuadamente son las copias de seguridad. Por lo tanto para la planeación de una política de copias de seguridad se deben tener en cuenta las siguientes consideraciones:

- Revisar que las copias de seguridad realizadas funcionen correctamente.

Esto implicaría restaurar una copia completa para asegurarnos que todo esta bien, pero este procedimiento sería demasiado engorroso por lo métodos habituales de operación, en lugar de esto, se pueden recuperar varios ficheros aleatorios del backup en tal forma que si esta operación funciona, se asumiría toda la copia como correcta.

- Marcar o etiquetar los backups en forma tal que un administrador pueda conocer la situación exacta de cada fichero, pero en cambio, para un atacante que roba el medio de almacenamiento le deberá ser difícil saber el contenido y orden del mismo; para conseguirlo se utilizan códigos impresos en cada etiqueta, códigos cuyo significado o simbología sea sólo conocido por los directamente responsables más no por un potencial atacante. Tenga en cuenta que si una etiqueta contiene información muy detallada acerca del contenido de una copia, esto sería peligroso porque si un atacante consigue sustraer una copia, no tendría mucha dificultad en conocer el contenido exacto, ya que le brindaría acceso a información concreta (y muy valiosa) a nuestros sistemas sin necesidad de mayores maniobras de penetración.
- El sitio donde se guardan las copias de seguridad es un aspecto muy importante y delicado, debido a que si se guardan en el mismo sitio de los sistemas no sería muy aconsejable debido a la posibilidad de ocurrencia de un desastre del entorno, como una inundación o un incendio, en los que se pueda perder tanto el sistema como las copias que pudieran ayudar a su recuperación. Por lo tanto una buena política de ubicación de backups será la que mantenga un juego de copias de seguridad completas en lugares diferentes a la sala de operaciones, pero protegido y aislado como ésta, y un juego de uso diario en la propia sala, con el fin de facilitar a los operadores la tarea de recuperación de ficheros; se recomienda también utilizar armarios ignífugos que necesiten de ciertas combinaciones para su apertura (combinaciones que sólo determinado personal ha de conocer), si se decide almacenar todos los backups en la mismo lugar que los equipos.

- Realizar copias de seguridad de los archivos que son únicos en nuestro sistema como:

✓ Las Bases de Datos.

✓ Directorios como /etc/, /usr/local, y directorios de usuario (dependiendo del Unix utilizado, /export/home, /users/, /home).

El hecho de realizar copias de seguridad a directorios como /dev/ o /proc/ no tiene objeto, así como tampoco realizar backups a directorios del sistema como /bin/ o /lib/, debido a que su contenido está almacenado en la distribución original del sistema operativo (por ejemplo, los CD-ROMs de instalación).

- **Cuándo se ejecutará el proceso**: En forma continuada y permanente.
- **Lo que se espera que suceda durante la ejecución del proceso:** Controlar la posibilidad de alteración, divulgación, modificación, interceptación, pérdida total o parcial de los datos.
- **Lo que no se espera que suceda:** Eliminar totalmente el riego de alteración, divulgación, modificación, interceptación, pérdida total o parcial de los datos.
- **Las acciones que se tomarán si ocurre un hecho imprevisto**: Rescatar los backups hasta la fecha más reciente, recurrir a los planes de contingencia.

- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas los mecanismos de recuperación respondan adecuadamente.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos

- **Qué se hará si se presenta un problema en el proceso:** Rescatar backups hasta la fecha más reciente, recurrir a planes de contingencia para minimizar el efecto.

Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**

NOMBRE DEL PROCEDIMIENTO:

Protección contra la amenaza que puede ocasionar un atacante interno, sistema de autenticación de Unix, revelado de contraseñas.

Observaciones: Evita – amenaza27.

Atacante Interno, sistema de autenticación de Unix, revelado de contraseñas.

Tipo Procedimiento (P: Preventivo, C: Correctivo): P,C

Propósito del procedimiento:

- **Qué estándar cumple:** A-1-1.1, A1-1.2, A-2-2.3, A.-2-2.5, A-2-2.7, B-2-2.2, B-2-2.2, B-4-4.3, B-5-5.3, C-2-2.1, C-3-3.12, C-3-3.14, C-3-3.15, D-4-4.1, D-4-4.3, G-1-1.1, G-1-1.2, G-2-2.4.3, H-1-1.1.5, H-1-1.1.6, H-1-1.1.7, H-1-1.1.9, H-1-1.1.10, H-1-1.3.2, H-1-1.3.3, H-1-1.3.4, H-1-1.3.5, H-1-1.3.6, H-1-1.3.7, H-1-1.3.8, H-1-1.3.9, H-1-1.3.10, H-1-1.3.11, H-1-1.3.12, H-1-1.3.13, H-1-1.3.14, H-1-1.3.15, H-2-2.3

Cuál es el objetivo del procedimiento: Los fraudes, robos sabotajes o accidentes relacionados con los sistemas informáticos son provocados por el propio personal de la organización dueña de dichos sistemas. Por lo tanto la mayor amenaza a los equipos de la organización surge principalmente por parte personas que trabajan o han trabajado para la misma. Es así como las personas que han trabajado con los administradores o programadores de una organización pueden llegar a conocer el sistema perfectamente, sus fortalezas y debilidades; por lo tanto un ataque realizado por esa persona va a ser probablemente un ataque mucho más peligroso porque puede ser más directo, difícil de detectar, y efectivo, que el que pueda propiciar un atacante externo que necesita recopilar información, intentar probar fallos de seguridad o conseguir privilegios para poder ejecutarlo. Si analizamos la motivación que pueda tener una persona para atacar su propia organización son diversos, ya que pueden ser económicos, inconformidad con el cargo, desafío personal, etc, la realidad es que este tipo de ataques ocurren y son muy frecuentes. Por tal motivo este procedimiento ha sido diseñado.

Alcance del procedimiento

- **A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento:** Puntos críticos de la red, canales de datos, sistemas de Bases de Datos, los sistemas y servidores de la D.S.I de la UIS.
- **Qué función se espera que este proceso ejecute**: Evitar un revelado de contraseñas por parte de un atacante interno.
- **Los conocimientos previos que se necesitan tener para ejecutar el proceso:** Conocimientos en encriptamiento o cifrado a nivel de hardware y software.

Definición del proceso

- **Introducción al proceso:** En los sistemas Unix cada usuario para acceder al sistema posee un nombre de entrada o login y una clave o password; los cuales se almacenan por lo general en el fichero /etc/passwd. Dicho archivo contiene una línea por usuario que contiene la información necesaria para que los usuarios puedan conectar al sistema y trabajar en él. Los campos son separados mediante el carácter ":". En el fichero /etc/passwd se encuentran entradas como las siguientes:

publico:x:1500:100:PUBLICO:/disco2/biblio:/bin/sh

En la que el primer campo aparece el login del usuario y su clave cifrada; luego el tercer campo el identificador de usuario, el cuarto campo el identifcador del grupo respectivamente, el quinto campo es conocido como GECOS contiene información administrativa sobre la identidad real del usuario como su nombre o teléfono. Finalmente los dos últimos campos corresponden al directorio del usuario ($HOME) y al shell que le ha sido asignado.

- **Descripción de lo qué el proceso hace:** El sistema operativo unix no diferencia a sus usuarios por su nombre de entrada al sistema, sino por medio del UID del usuario; el login es empleado más bien por comodidad de los usuarios ya que es más fácil de recordar que un UID, principalmente si se tienen cuentas en muchas máquinas, cada una con un UID diferente, pero si en /etc/passwd llegan a existir dos entradas con el mismo UID, Unix los tomaría como el mismo usuario, aunque tengan un login y password diferente: por lo tanto si dos usuarios tienen asignado el UID 0, ambos tendrán privilegios de superusuario, sin importar el login que utilicen. Esta situación es aprovechado por atacantes que logran conseguir privilegios de administrador en una máquina, logrando añadir una línea a /etc/passwd con un nombre de usuario normal pero con el UID 0; garantizando con esta maniobra la entrada al sistema como administradores, en caso de ser descubiertos, para borrar los rastros o huellas. La detección de esta línea es difícil especialmente en sistemas con gran números de usuarios, pero para detectar las cuentas con privilegios en la máquina se puede utilizar el comando: awk –F:'$3==0 {print $1}' /etc/passwd.

Respecto a los ataques de texto cifrado escogido estos conforman la principal amenaza al sistema de autenticación de Unix; aunque no es posible descifrar una contraseña, si es fácil cifrar una palabra junto a un determinado salt, y comparar el resultado con la cadena almacenada en el fichero de claves, generalmente ubicado en /etc/passwd. De esta manera, el atacante leerá el fichero de claves y luego empleará un programa adivinador de contraseñas conocido también como crackeador, el cual cifrará todas las palabras de un fichero denominado diccionario, comparando los resultados obtenidos en este proceso con la clave cifrada del fichero de contraseñas, si los resultados coinciden el atacante ha obtenido una clave para acceder al sistema.

- **Cómo se ejecutará el proceso:** Dentro de las medidas de prevención que

se pueden tomar contra atacantes internos se deben tener en cuenta las siguientes:

- Revisar con sumo cuidado las hojas de vidas de los aspirantes a cargos dentro de las organizaciones, investigando su pasado laboral.
- Otorgar los mínimos privilegios que necesiten para desempeñar adecuadamente sus cargos.
- Conocimiento parcial. Las actividades más delicadas de seguridad informática dentro de la organización como por ejemplo: el conocimiento de la clave de root de una máquina deben ser efectuadas por dos personas competentes, esto con el fin de garantizar que si uno de los responsables no está presente, el otro puede seguir operando los sistemas sin inconveniente alguno mientras que el otro compañero supera las dificultades acaecidas.
- Rotación de funciones. La posible complicidad que pueda surgir por los dos responsables de cierto trabajo, en tal forma que los dos sean capaces de ocultar las violaciones de seguridad o que suceda lo contrario, es decir, que ambas estén en desacuerdo repercutiendo en el buen funcionamiento de la política de seguridad establecida, para evitar estos inconvenientes se recomienda rotar a las personas en las diferentes responsabilidades, con el objetivo que a la larga todos puedan vigilar a todos, trayendo un beneficio adicional que es en el caso de que alguno de los responsables abandone la organización, las tareas pueden ser cubiertas más fácilmente.
- Separación de funciones. No es recomendable que una sola persona posea demasiada información acerca de la seguridad de la organización, por lo tanto es necesario definir y separar adecuadamente las funciones de cada persona, en tal forma que si alguien tiene la tarea de controlar la seguridad de un sistema, no posea la capacidad de violarla sin que nadie se percate de ello.
- Al abandonar una persona la organización, se le debe cancelar inmediatamente el acceso a todos los recursos como por ejemplo cuentas de usuario, servicio de acceso remoto, unidades de red, y cambiar las claves que el usuario conocía. En entornos de gran movilidad de usuarios como lo es una Universidad, es difícil aplicar esta medida (un profesor invitado durante un mes, un estudiante que sólo necesita acceso a una máquina mientras culmina su proyecto, entre otros) por lo que en estas situaciones se presentan casos como: cuentas que hace años no se utilizan, direcciones de correo de personas que dejaron de trabajar para la organización hace tiempo. Todas estas circunstancias pueden amenazar la seguridad del sistema y pueden ser aprovechadas por un atacante para obtener puertas de acceso o entrada al sistema de la organización.
- Respecto a la universidad, las normas referidas anteriormente son orientadas especialmente sobre el personal empleado o contratado por la organización, pero no sobre los alumnos, que son los principales factores de ataques en la universidad, la cual, debe preocuparse por diseñar otras medidas de prevención, como por ejemplo: sanciones a los que utilicen los recursos del alma mater para realizar maniobras informáticas ilegales. Las sanciones pueden resultar siendo buenas medidas de coacción para evitar ataques por parte de los estudiantes.

El sistema de autenticación de Unix no está exento de debilidades, para controlarlas se pueden tomar las siguientes medidas de protección:

- Para evitar ataques de texto cifrado escogido se deben emplear passwords que no sean palabras fáciles de adivinar o que pertenezcan a ficheros de diccionarios típicos. No es aconsejable escoger claves sencillas como nombres de personas, combinaciones simples como juan01, nombres de actores, lugares, mascotas, animales, etc, en cambio es recomendable emplear combinaciones de mayúsculas con minúsculas, símbolos como $,*,&, etc, lo mismo que texto mezclados con números. Para evitar passwords fáciles de adivinar se han hecho estudios y se han diseñado fuertes herramientas como Passwd+ o Npasswd, las cuales se recomiendan sean utilizadas para forzar a los usuarios a emplear contraseñas adecuadas. A pesar de estas medidas, un administrador no se puede confiar, y debe ejecutar con alguna periodicidad algún programa adivinador de contraseñas, tipo Crack, para verificar que los usuarios no han escogido contraseñas débiles. Se debe insistir a los usuarios, acerca de la importancia de mantener las contraseñas en total secreto, por muy elaboradas que sean, pierden toda la robustez si es compartida con otros usuarios.

Hoy en día los usuarios tienen la posibilidad de instalar en sus equipos personales aplicaciones software orientadas a la generación automática de claves, no crackeables. Estas herramientas le evitan al usuario tener que recordar o memorizar sus claves, situación que es bastante molesta para él y en especial cuando posee varias cuentas en varios equipos y sitios web. Dentro de estas herramientas encontramos a Password Depot, la cual está disponible gratuitamente en http://www.password-depot.com, la cual permite salvar todos los passwords de las diferentes cuentas en una sola lista, además permite generar claves inviolables o “incrackeables” debido a que contiene en su generador de passwords algoritmos robustos de encripción, tales como Blowfish y Rijndael; el usuario no necesita recordar las contraseñas o passwords ya que el software le permite insertar las claves en donde las necesita con sólo arrastrarlas y soltándolas con el mouse.

- Oscurecimiento de contraseñas (Shadow Password). Técnica empleada para proteger las contraseñas de los usuarios. Su funcionamiento en esencia trata de impedir que los usuarios sin privilegios puedan leer el archivo o fichero que almacena las claves cifradas. El archivo /etc/passwd debe tener permiso para ser leído por todos si se desea que el sistema funcione adecuadamente. Cuando se emplea la técnica de oscurecimiento de contraseñas, el fichero continúa siendo legible para todos los usuarios, pero la diferencia radica en que con este procedimiento las claves cifradas ya no se guardan en el fichero /etc/passwd, sino en el archivo /etc/shadow, que sólo el root puede leer. En el campo correspondiente a la clave cifrada de /etc/passwd ya no aparece ésta, sino un símbolo por lo general una “x” que significa en algunos programas como /bin/login las claves deben ser buscadas en /etc/shadow. En cuanto a la presentación, el fichero /etc/shadow es similar al de /etc/passwd/, ya que contiene una línea por cada usuario del sistema en donde se almacena cada login y su respectiva clave cifrada; el resto de campos de este fichero varían, y contienen información que permite implementar otro mecanismo para proteger

las claves de los usuarios: el envejecimiento de contraseñas o Aging Password. La mayoría de sistemas Unix en el mercado tienen incorporado este mecanismo, y se puede comprobar si lo contiene si al instalar el sistema operativo este contiene las claves en /etc/passwd y acepta la orden pwconv que convierte un sistema clásico en uno oscurecido. Si el sistema es muy antiguo y no soporta el mecanismo Shadow Password, se recomienda instalarlo: shadow.tar.gz, el cual se encuentra disponible en varios servidores.

- Envejecimiento de contraseñas (Aging Password). Técnica basada en la protección de passwords de los usuarios asignándoles un determinado periodo de vida, es decir la contraseña sólo va a ser válida durante un lapso de tiempo, el cual al expirar obligará al usuario a cambiarla.

El periodo de expiración de las claves es establecido en el momento de crear los usuarios con las diferentes herramientas que los sistemas ofrecen. En caso de querer modificar los períodos de tiempos establecidos, se pueden cambiar desde estas mismas herramientas de administración, como también desde la línea de comandos con órdenes como usermod o chage. Si un usuario decide cambiar su clave, el mismo sistema le impide volverla a cambiar durante un lapso de tiempo, esto con el objetivo de que cuando el sistema exija volver a cambiar la contraseña, el usuario no vuelva a restaurar su clave antigua, además si se cumple el período de cambio obligatorio de contraseña y el usuario no lo hace, el sistema le bloquea la cuenta.

- Claves de un solo uso. El envejecimiento de contraseñas puede seguir dos formas de actuación:

La primera es utilizar el esquema clásico, en la cual una clave es válida hasta que el mismo usuario decida cambiarla, es decir la contraseña no caduca. El segundo es el esquema Aging Password, el cual actúa otorgando un tiempo de vida mínimo a cada clave, de manera que sólo sirva para una conexión, método también llamado clave de un solo uso (One Time Password). Un sistema que aplica esta técnica de clave de un solo uso es el que utiliza un pequeño dispositivo que puede ser una calculadora o una tarjeta, la cual es portada por el mismo usuario, de forma que cuando se desee conectar al sistema este dispositivo le indica una secuencia de caracteres o en otras palabras la clave a teclear para acceder al sistema. En caso de ser robada la tarjeta o calculadora es posible mejorar la seguridad utilizando un P.I.N que el usuario debe mantener en secreto antes de digitar la contraseña emitida por el dispositivo (calculadora o tarjeta). Una aplicación One Time Password muy extendida entre varios clones Unix es S/Key, que también está disponible para clientes tanto Windows como MacOS. Al emplear este software, la clave de los usuarios nunca viaja por la red, ni siquiera al ejecutar órdenes como **su** o **passwd**, tampoco es almacenada información comprometedora como claves en claro en la máquina servidora.

- PAM (Pluggable Authentication Module). No es propiamente un modelo de autenticación, sino mas bien un mecanismo que brinda una interfaz entre las aplicaciones de usuario y diferentes métodos de autenticación. Pretende solucionar uno de los problemas clásicos de la autenticación de usuarios, el cual consiste en que una vez se ha elegido e implantado algún mecanismo de autenticación en un entorno, y luego se desea cambiarlo resulta complicado

cambiarlo. Por lo tanto PAM permite comunicar las aplicaciones con los métodos de autenticación deseados de una forma transparente, permitiendo integrar las utilidades de un sistema Unix clásico (login,ftp,telnet) con esquemas diferentes del habitual password: claves de un solo uso, tarjetas inteligentes, etc.

Al analizar el fichero de configuración de PAM (/etc/pam.conf) está conformado en la siguiente forma: servicio tipo control ruta_modulo argumentos_modulo. Donde "servicio" se refiere al nombre del servicio sobre el que se aplica la autenticación, puede ser ftp, telnet, passwd; el campo "tipo" especifica el tipo de servicio sobre el que se aplica el módulo; en el campo "control" se define que hacer ante el éxito o el fracaso del módulo afectado. Por último el campo "ruta_modulo" indica el nombre del módulo o mejor la ruta donde está ubicado el fichero, además el campo "argumentos_modulo" se refiere a los argumentos que se han de pasar cuando se invoca, siendo además el único campo opcional del fichero. Generalmente en implementaciones más modernas como las de Linux, la configuración de PAM se encuentra distribuida en los diferentes ficheros dentro del directorio /etc/pam.d/, en la que el nombre de cada fichero define el servicio al que afecta la autenticación (en la que se encuentran archivos como "ftp", "telnet" entre otros), por tanto las líneas de cada fichero sólo tienen las cuatro últimos campos expuestos anteriormente.

En conclusión, PAM brinda soluciones a los diferentes problemas de autenticación de usuarios en entornos Unix, ya que proporciona independencia entre los servicios del sistema y las técnicas de autenticación empleadas, lográndose convertir en un estándar de autenticación dentro de entornos Unix.

- **Cuándo se ejecutará el proceso**: En forma continuada y permanente.
- **Lo que se espera que suceda durante la ejecución del proceso:** Controlar la posibilidad de ocurrencia de un revelado de contraseñas por parte de un atacante interno.
- **Lo que no se espera que suceda:** Que un intruso logre mediante alguna maniobra un revelado de contraseñas.
- **Las acciones que se tomarán si ocurre un hecho imprevisto**: Revisar los sistemas de protección de contraseñas.
- **Qué criterios indican la ejecución exitosa del proceso:** Que al efectuar pruebas no se logren revelar contraseñas.
- **Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará:** Enviar un formato informe acerca del procedimiento efectuado, el cual lo debe llenar el Coordinador Funcional de Seguridad Informática, quién anexará el visto bueno del Director Funcional (Director de Escuela), para luego ser entregado al Coordinador de Seguridad Informática, quién enviará un reporte-informe de inconvenientes de seguridad mensual o como se estime conveniente al Director De Seguridad Informática que lo compartirá o analizará con el Comité de Seguridad Informática
- **Las interacciones requeridas o esperadas de otros procesos:** Ninguna

Problemas de los procesos • **Qué se hará si se presenta un problema en el proceso:** Revisar las herramientas de protección de contraseñas.	
Excepción del proceso por no aplicabilidad: Ninguna	**Responsable:**