UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"ANÁLISIS DE RIESGO A 7 DEPARTAMENTOS DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

CABALLERO SANTILLÁN VALERIA

MORENO MENDOZA FRANCISCO XAVIER

PEREA SÁNCHEZ ROGELIO ABEL

DIRECTORA DE TESIS:
M.C. CINTIA QUEZADA REYES

MÉXICO D.F. 2009

VALERIA

José Luis y Marina mis padres, agradezco sus enseñanzas, amor, logros profesionales, pero sobre todo, la increíble experiencia de estar viva.

A Adriana, a quien agradezco todos los cuidados, apoyo incondicional y ese gran espíritu de hermandad y protección.

A Samantha por haber llegado a mi vida.

A Enrique por su fiel amistad y enseñanzas académicas.

A Lile, Dora y Oscar mis amigos del alma por los momentos inolvidables vividos con lagrimas y alegrías.

A la M.C. Cintia Quezada Reyas por el apoyo en la elaboración de esta tesis.

Agradecimientos

FRANCISCO XAVIER

Me resulta muy difícil expresar en unas cuantas palabras el agradecimiento que tengo hacia muchas personas, pero existen personas muy importantes en mi vida que me apoyaron en todo este proceso.

A mis padres: No tengo palabras para agradecer todo el apoyo que me dieron en toda mi vida escolar, como también agradezco su cariño, consejos, amor y comprensión que tuvieron hacia mí, ya que sí tuvieron demasiada paciencia para poder entenderme.

A mi hermano: Le agradezco su apoyo, comprensión y ayuda en problemas que tuvimos a lo largo de nuestras vidas. Espero ver pronto tu examen profesional también.

A mis tíos: Agradezco a todos mis tíos, es muy difícil mencionar a cada uno, ya que sabemos la cantidad que somos. Les doy gracias por su apoyo y consejos a lo largo de toda esta vida.

A mis primos: Les agradezco tantos días de fiestas, felicidad y consejos que me han dado a lo largo de mi vida.

A mis amigos: No sé como agradecer todo el apoyo, ayuda y tantas fiestas y diversiones que me dieron a lo largo de mi vida universitaria, saben que se les quiere mucho.

A mis profesores: Les agradezco por proporcionarme todos esos conocimientos que me ayudaron a lo largo de la vida universitaria. Así como enseñarme los buenos valores en la vida. En especial le agradezco a la M.C. Cintia Quezada Reyes y al Ing. Orlando Zaldívar Zamorategui, por su apoyo tanto en el proceso de titulación como en mi trayectoria escolar.

Agradecimientos

ABEL

Esta tesis representa la culminación de mi carrera en la Facultad de Ingeniería y quiero agradecer a quien contribuyó a que tuviera la energía para completar este ciclo.

A mis padres por siempre brindarme su apoyo y simplemente estar ahí cuando los necesité; igualmente gracias por el apoyo al resto de mi familia.

A todas las personas que conocí en esta facultad, y que ahora son mis amigos, su amistad es algo que no olvidaré.

A mis mejores amigos de siempre, saben que ustedes siempre ayudan (¡¡¡venga CUM !!!).

A los profesores, de alguna u otra manera aprendí algo de ellos.

A la M.C. Cintia Quezada Reyes, quien nos ofreció la gran oportunidad de titularnos y nos dio su confianza y apoyo durante el proceso.

A todas las bebidas, de todo tipo, consumidas durante toda la carrera.

Un placer haber estudiado en esta universidad. Gracias.

INDICE

CAPÍTULO 4 ANÁLISIS DE RIESGO

CAPÍTULO 5 ANÁLISIS DE RIESGO DE LOS SIETE DEPARTAMENTOS.

INTRODUCCIÓN

INTRODUCCIÓN

El acelerado crecimiento de la tecnología en los últimos años ha generado un creciente número de oportunidades así como un creciente número de amenazas. Dado el aumento de estas amenazas, se tiene la necesidad de hacer un análisis exhaustivo sobre el riesgo o pérdida que pueden sufrir los bienes dentro de una organización para que de esta manera se puedan mitigar oportunamente los daños y las pérdidas totales o parciales que puedan generarse.

Garantizar que los recursos informáticos de una compañía no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de Seguridad Informática.

En términos generales la Seguridad Informática determina:

- ¿Qué necesita ser protegido y por qué?
- ¿De qué necesita protegerse?
- ¿Cómo se va a proteger mientras exista?

Para tratar de minimizar los efectos de un problema de seguridad se realizó el análisis de riesgos a siete departamentos de una organización. Como metodología de diagnóstico para poder establecer la exposición a los riesgos por parte de la organización, se recurre al análisis de riesgo.

El análisis de riesgo utilizado es de tipo cualitativo ya que trata una estimación de pérdidas potenciales, esto se logra interrelacionando cuatro elementos principales: las amenazas (siempre presentes en cualquier sistema), las vulnerabilidades (que potencian el efecto de las amenazas), el impacto asociado a una amenaza (que indica los daños sobre un activo por la materialización de dicha amenaza) y los controles (contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos)).

El trabajo se encuentra conformado de la siguiente manera:

En el capítulo I se mencionan conceptos generales acerca de la seguridad informática.

Continuando con el capítulo II se hace referencia a los servicios de seguridad existentes, los cuales son de importancia para el análisis de riesgo.

Dentro del capítulo III se mencionan algunas herramientas de seguridad las cuales son importantes para establecer un sistema de protección en los sistemas informáticos en la institución.

En el capítulo IV se define lo que es un análisis de riesgo, así como los pasos que lo integran.

Finalmente, el capítulo V contiene el análisis de riesgo realizado a los siete departamentos de una institución. En éste puede observarse lo que se menciona a continuación:

1. Definición del alcance que tendrá el análisis de riesgos en la institución.

2. Elaboración de cuestionarios y entrevistas que serán aplicados al personal que labora en los siete departamentos de la institución que abarquen el análisis de riesgo y que permitan reconocer activos, así como vulnerabilidades y amenazas.

3. Inspección de instalaciones de la institución pertenecientes a los siete departamentos que permiten seguir reconociendo los activos y las distintas amenazas y vulnerabilidades del lugar.

4. Recolección de evidencia.

5. Análisis en forma de la evidencia obtenida en los cuestionarios y la inspección a los departamentos de la institución asignados para este análisis.

6. Análisis de controles existentes en los distintos departamentos

7. Planteamiento de recomendaciones.

8. Elaboración del informe que constituye el análisis de riesgo donde se plasman los resultados obtenidos así como las recomendaciones necesarias para cada área.

CAPÍTULO 1

Conceptos Generales

1.1 DEFINICIÓN DE SEGURIDAD INFORMÁTICA

Se puede entender como seguridad un estado de cualquier sistema (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

Se puede definir información como el conocimiento obtenido a partir de la investigación, el estudio o instrucción, inteligencia, noticias, hechos, datos, una señal o carácter (como un sistema de comunicación o computadora) representando datos, algo (como mensaje, datos experimentales o una imagen) que justifique el cambio en una construcción (como un plan o una teoría) que representa la experiencia física o mental u otra construcción.

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible para las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La seguridad informática debe proteger todos los activos de una organización. Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Los activos están conformados por tres elementos:

a) Información

Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, puede ser en algún medio electrónico o físico.

b) Equipos que la soportan

Software, hardware y organización.

c) Usuarios

Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- Integridad: La información sólo puede ser modificada por quien está autorizado para hacerlo. La integridad se refiere a la seguridad de que la

información no ha sido alterada, borrada, reordenada, copiada, etcétera, ya sea durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descriptar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

- Confidencialidad: La información sólo debe ser legible para los procesos o el personal autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada, las líneas "intervenidas", la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

- Disponibilidad: Debe estar disponible cuando se necesita. La disponibilidad de la información se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

- Irrefutabilidad o identidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría de cierta actividad. Garantiza que la identidad o responsabilidad de un evento corresponde a un actor específico generador de dicho evento.

Otras características importantes de seguridad son la autenticación, es decir, la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser y los controles de acceso, esto es, quién tiene autorización y quién no para acceder a una parte de la información.

Finalmente se tiene el problema de la verificación de la propiedad de la información, es decir, que una vez que se ha detectado un fraude, determinar la procedencia de la información.

El objetivo de la seguridad informática es preservar los activos de una organización y mantener su operación, basado en las características anteriores.

El contexto general de la seguridad así como su ciclo administrativo y sus relaciones se pueden apreciar en los siguientes diagramas (Figura 1.1 y 1.2):

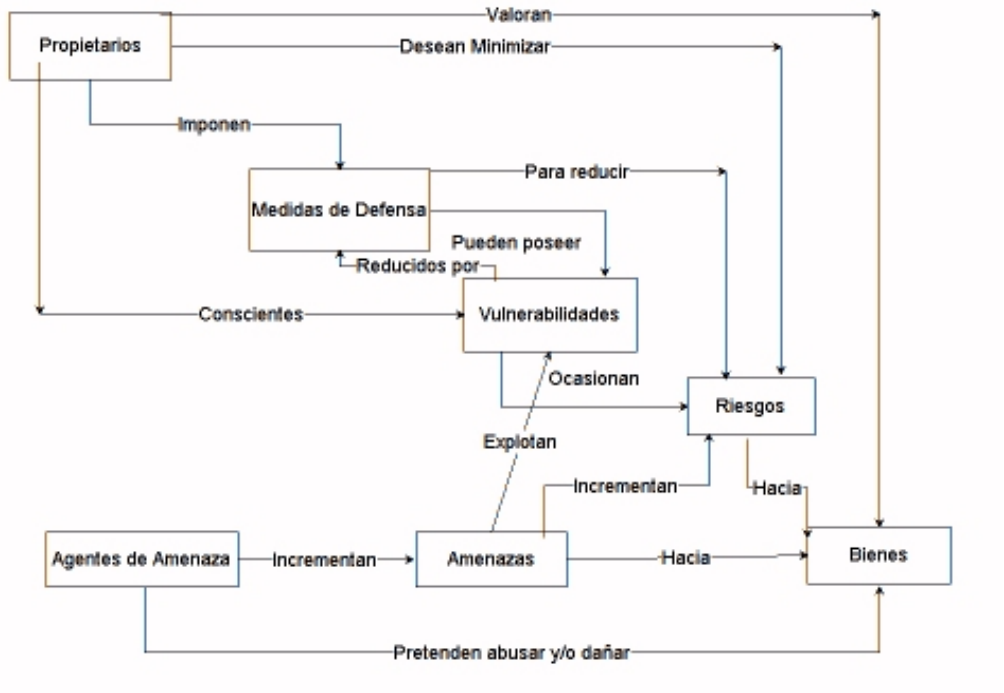


Figura 1.1 Contexto de la seguridad informática y sus relaciones

Figura 1.2 Ciclo de administración de la seguridad

Debido a que la seguridad no existe al 100%, es necesario que la seguridad se vea como un ciclo, para que exista un constante resguardo de la información. El ciclo se resume en planear, proteger, detectar y reaccionar porque es la estrategia que da constancia y continuidad a la seguridad en una organización y permite modificar y mejorar siempre que sea necesario. La seguridad requiere de una

supervisión continua, no es una acción estática debido a que las actividades en una organización son dinámicas ya que cambian constantemente, así como quienes forman parte de la misma.

En mayor o menor grado, todo sistema necesita seguridad. En una primera aproximación, para determinar cuál es la seguridad adecuada en un sistema habrá que estudiar cuáles son los riesgos a los que se está expuesto, teniendo en cuenta el valor de la información que contiene, los costos de recuperación ante un hipotético incidente y por supuesto evaluar lo que costaría la protección. Las amenazas y las vulnerabilidades ocasionan e incrementan los riesgos por lo que es importante saber en qué consisten.

1.2 AMENAZAS

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben tomarse en cuenta circunstancias que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables.

Una amenaza es todo aquello que puede, intenta o pretende destruir o dañar los activos en una organización. La amenaza es un evento que puede desencadenar un incidente en la organización, se encentra como peligro latente y puede o no llegar a manifestarse.

1.2.1 TIPOS DE AMENAZAS

Las amenazas surgen de distintas fuentes por lo que las podemos clasificar en cinco tipos:

a) Humanas: Surgen por la ignorancia, descuido, negligencia y hasta inconformidad por parte de algún usuario en el manejo de la información. Este tipo de amenaza incluye:

- Ingeniería social: Es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían. Con esta práctica se puede obtener información confidencial a través de la manipulación de usuarios legítimos.

- Robo: Puesto que el robo, normalmente no supone la destrucción de la información original, sus consecuencias serán de tipo económica, tácticas o quizás una amenaza contra la intimidad de las personas.

- Sabotaje: Puede estar dirigido contra la información (en forma de destrucción o manipulación) o también tener como objetivo la destrucción de los equipos, por lo que puede afectar tanto a la disponibilidad del sistema como la integridad de la información contenida.

- Fraude: Consiste en manipular la información con el fin de obtener un beneficio.

- Intrusos remunerados: Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o script boy, viruxer, etcétera).

- Personal interno: Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

- Terrorismo: Actos que atentan contra la información para causar diversos daños a los usuarios, manipulando o eliminando información.

b) Errores de hardware: Son las fallas físicas que pueden existir en los dispositivos que conforman un sistema. Este tipo de errores afectan a la disponibilidad del sistema pudiendo provocar también una pérdida de información.

c) Errores de la red: Significa tener problemas debido al mal diseño e implementación de la red en una organización. Cuando se presentan estos errores no existe un buen flujo de información provocando problemas de disponibilidad.

d) Problemas de tipo lógico o errores de software: Suceden cuando los mecanismos de seguridad no están correctamente implementados en un sistema, provocando que diversos programas maliciosos puedan penetrar y causar daños en la información; así como también el sistema de la organización puede sufrir un mal funcionamiento. Los programas maliciosos son destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o spyware.

e) Naturales: Los desastres naturales como inundaciones, fuego, terremotos, etcétera, suelen tener consecuencias serias para los sistemas; tales como daños en los equipos, pérdida de información y no disponibilidad. La ubicación territorial es un factor muy importante que determina el riesgo que se corre frente a cada desastre. Por ejemplo, al igual que en una zona sísmica el riesgo de terremoto es alto, en un lugar seco rodeado de árboles

es mayor el de incendio. A este tipo de amenazas también se les conoce como actos de Dios.

Seguridad se podría definir como todo aquello que permite defenderse de una amenaza. Se considera que algo es o está seguro si ninguna amenaza se cierne sobre ello o bien el riesgo de que las existentes lleguen a materializarse es despreciable, lo cual pocas veces se podrá afirmar de forma tajante, sea cual sea la naturaleza de lo que se esté hablando.

1.3 VULNERABILIDADES

Por vulnerabilidad se entiende la exposición latente a un riesgo, el punto de un sistema que puede ser dañado. Las vulnerabilidades abarcan todo lo que se deja de hacer en una organización, todo lo que no se considera, lo que no se estudia, lo que no se aplica, etcétera. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y ahora, las empresas deben enfrentar amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos, es decir la consumación de una amenaza.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes con la importancia de la información en riesgo.

1.3.1 TIPOS DE VULNERABILIDADES

Las vulnerabilidades pueden ser de tipo:

- Natural: Problemas con desastres naturales o ambientales, por ejemplo, el no contar con extinguidores en caso de incendio o la construcción en zonas de alto riesgo sísmico debido a la falta de un análisis previo.

- Física: Problemas con el acceso a las instalaciones e incluso a los equipos que contienen información que se busca proteger. Por ejemplo:

- Acceso físico a los equipos informáticos sin control alguno
- Acceso a los medios de transmisión (cables, ondas,..) sin previa autorización.

- Lógica: programas o algoritmos que puedan alterar el almacenamiento, acceso, transmisión, etcétera; por ejemplo errores de programación y diseño debido a que no se siguieron metodologías o no se llevaron a cabo pruebas necesarias.

- Hardware: Problemas con los equipos, por ejemplo, el evitar leer los manuales de los dispositivos y no tomar en cuenta sus características para un funcionamiento óptimo.

- Red: Fallas con la red de la organización, por ejemplo, una mala administración de la red o un mal diseño debido al incumplimiento de estándares internacionales.

- Humana: Las personas que administran y utilizan el sistema constituyen la mayor vulnerabilidad del sistema.
  - Toda la seguridad del sistema descansa sobre el administrador, o administradores.
  - Los usuarios también suponen un gran riesgo debido a descuidos, negligencia, ignorancia, revanchas, etcétera.

La única lucha contra estas vulnerabilidades es la implantación de sistemas de seguridad.

1.4 ATAQUES

Los ataques son todas aquellas acciones o eventos, exitosos o no, que atentan sobre el buen funcionamiento del sistema, es decir, atentan contra la confidencialidad, integridad o disponibilidad del sistema informático.

Un ataque es la realización de una amenaza tras explotar una o varias vulnerabilidades

Las cuatro categorías generales de ataques en redes toman en cuenta el flujo normal para el envío de la información, en donde se ven involucrados un emisor y un receptor de información. Estas categorías son:

- Interrupción: Es un ataque contra la disponibilidad en donde el receptor no recibe la información del emisor. Se puede presentar, por ejemplo, al desconectarse el cable de red en un equipo.

- Suplantación: Es un ataque contra la autenticación en donde una tercera entidad llamada perpetrador aparece entre el emisor y el receptor, haciendo que éste último tenga contacto con la entidad maliciosa y no con el verdadero emisor de información. Por ejemplo, las páginas falsas en Internet.

- Intercepción: Ataque contra la confidencialidad en donde un perpetrador consigue la información que es enviada de emisor a receptor. Por ejemplo, programas que capturan contraseñas.

- Modificación: Ataque contra la integridad. En este caso, la información pasa por el perpetrador antes de llegar con el emisor, por lo que puede sufrir cambios o daños. Por ejemplo, la modificación de imágenes.

1.4.1 TIPOS DE ATAQUES

Las cuatro categorías antes mencionadas pueden dividirse en dos tipos de ataques: pasivos y activos, esto con base en la manipulación de la información.

a) Ataques pasivos

En los ataques pasivos el atacante (perpetrador, oponente o persona que se entromete al sistema) observa, escucha, obtiene o monitorea mientras la información está siendo transmitida, es decir, no altera en ningún momento la información.

Los principales objetivos del atacante pasivo son:

- Intercepción de datos: En este caso, el atacante sólo tiene conocimiento del contenido de la información.

- Análisis de tráfico: Consiste en la observación de todo el tráfico de información que se transmite por la Red.

Con los ataques pasivos se logra la obtención del origen y destinatario de la comunicación (emisor y receptor), control de volumen de tráfico, es decir, se conoce la frecuencia y longitud de los mensajes además de que el perpetrador tiene el control de las horas habituales de intercambio de datos entre las entidades de comunicación.

Es muy difícil la detección de los ataques pasivos debido a que no se provoca ninguna alteración de los datos pero sí se pueden prevenir, para lograrlo es importante contar con mecanismos de cifrado de información, entre otros.

Dentro de este tipo de ataques podemos clasificar a la intercepción.

b) Ataques activos

En los ataques activos el atacante modifica la información, modifica la corriente de datos o incluso una interrupción o desvío de información.
Los ataques activos se clasifican de la siguiente manera:

- Enmascaramiento o suplantación de identidad: Es aquí donde el intruso se hace pasar por una entidad diferente.

- Replica o reactuación: En este caso, uno o varios mensajes legítimos son capturados y replicados para saturar al sistema.

- Modificación de mensajes: consiste en que la información original del mensaje transmitido, es alterada, provocando con esto un efecto no autorizado.

- Degradación del Servicio: en este ataque se inhibe o impide el uso normal de los recursos informáticos o de comunicaciones.

En los ataques activos como hay modificación de la información, es posible detectar estos ataques, aunque en algunos casos es demasiado tarde.

Dentro de este tipo de ataques podemos clasificar a la interrupción, la suplantación y la modificación.

CAPÍTULO 2

SERVICIOS DE SEGURIDAD

2.1 PANORAMA GENERAL

Los servicios de seguridad son acciones o actividades que mejoran e incrementan la seguridad de un sistema de información o el flujo de la información.

En complemento todas las actividades que permiten implementar un servicio de seguridad conforman un mecanismo de seguridad.

Cada mecanismo de seguridad está compuesto por herramientas (software y hardware) y por sus controles (reglas, estándares, recomendaciones, planes, medidas, buenas prácticas) y cada uno de éstos puede implementar uno o más servicios de seguridad.

2.2 TIPOS DE SERVICIOS DE SEGURIDAD INFORMÁTICA

El objetivo principal de los servicios de seguridad es mantener seguro un sistema de información haciendo frente a las amenazas de la seguridad del sistema.

Estos servicios hacen uso de uno o varios mecanismos de seguridad para proteger los sistemas de proceso de datos y de transferencia de información de una organización.

Existen 6 tipos de servicios de seguridad que pueden ser implementados con el fin de evitar ataques de seguridad. Los servicios son:

I. Confidencialidad.

II. Autenticación.

III. Integridad.

IV. No repudio.

V. Disponibilidad.

VI. Control de acceso.

2.2.1 CONFIDENCIALIDAD

La confidencialidad es un aspecto muy importante dentro de la seguridad informática, significa asegurar que sólo los individuos autorizados tengan acceso a

los recursos que se intercambian, es decir, previene la divulgación de información a personas o sistemas no autorizados y requiere que únicamente las entidades autorizadas puedan acceder a la información. Lo anterior es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadoras y datos residen en localidades diferentes, pero están física y lógicamente conectados.

La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez sólo porciones o segmentos seleccionados de los datos, por ejemplo, mediante el uso del cifrado.

Es importante hacer notar que los servicios de confidencialidad se basan en dos aspectos fundamentales, los cuales son:

I. La confidencialidad de flujo de tráfico, el cual protege la identidad del origen y destino(s) del mensaje, a través del cifrado con lo cual se oculta el flujo del mensaje y procura que la información se prevenga de una observación. De esta forma se intenta asegurar que nadie pueda interceptar las comunicaciones o los mensajes entre entidades.

II. La confidencialidad del contenido del mensaje utiliza una técnica de cifrado para prevenir el descubrimiento no autorizado del contenido del mensaje, un archivo o un registro de datos; con la finalidad de que el personal no autorizado pueda leer, copiar descubrir o modificar la información sin autorización.

Los métodos de cifrado de datos basados en la criptografía así como las buenas prácticas en el uso de contraseñas son mecanismos de confidencialidad, entre otros, para asegurar que personas no autorizadas tengan acceso a la información confidencial.

2.2.2 AUTENTICACIÓN

En la autenticación se asegura que sólo los individuos autorizados tengan acceso a los recursos. La autenticación consiste en la confirmación de la identidad de un usuario, es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser, requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa.

La seguridad informática se basa en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Se denomina identificación al momento en que el usuario o proceso se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esta identificación.

En otras palabras, el sistema verifica la información que alguien provee contra la información que el sistema sabe sobre esa persona o proceso.

Existen dos tipos de autenticación:

I. Autenticación de entidad: En ésta se asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etcétera), tarjetas de banda magnética, contraseñas, o procedimientos similares.

II. Autenticación de origen de información: Asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

La autenticación se lleva a cabo, basándose en cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- *Algo que solamente el individuo conoce:* En este caso puede ser una clave secreta de acceso o contraseña (conocida en inglés como password), una clave criptográfica, un número de identificación personal, etcétera. Cuando esta información es accedida al sistema, éste lo verifica contra la copia que está almacenada en el sistema para determinar si la autenticación es exitosa o no.

- *Algo que la persona posee*: Aquí entran cosas tangibles que se tienen, por ejemplo, un pasaporte o una tarjeta magnética, con esto el sistema verifica la identidad de quien lo posee y corrobora si es realmente quien dice ser.

- *Algo que el individuo es y que lo identifica unívocamente:* En este caso se autentica al individuo por factores únicos en él, los cuales se encuentran determinados genéticamente, puede ser la retina, la imagen del rostro, una huella digital o incluso la voz.

- *Algo que el individuo es capaz de hacer*: Se basa en las capacidades o habilidades del individuo que le permiten realizar ciertas actividades, por ejemplo, los patrones de escritura.

Para cada una de estas técnicas es importante mencionar que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por la dificultad para lograr su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina *"single login*" o sincronización de contraseñas.

Una de las posibles técnicas para implementar esta única identificación de usuarios (*"single login"*) sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

2.2.3 INTEGRIDAD

La integridad garantiza que los datos sean los mismos que eran inicialmente, porque no han presentado ningún tipo de alteración, es decir, la integridad requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación de los mensajes transmitidos buscando mantener los datos libres de modificaciones no autorizadas. La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente). Si la integridad no existe en un sistema, cualquier persona podría manipular los datos según su conveniencia.

La integridad puede aplicarse a una secuencia de mensajes o al contenido de un solo mensaje.

Un servicio de integridad de la secuencia de mensajes asegura que la secuencia de los bloques o unidades de mensajes recibidas no ha sido alterada y que no hay unidades repetidas o perdidas durante su transmisión. Por otro lado, el servicio de integridad del contenido de un solo mensaje asegura que los datos recibidos no han sido modificados de ninguna manera.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.

Algunos mecanismos de seguridad a través de los cuales se puede ofrecer integridad en los datos son:

- Message Authentication Code (o MAC): El código de autenticación del mensaje es un código que se genera a partir de un mensaje de longitud arbitraria y de una clave secreta compartida entre el remitente y el destinatario, es decir, se les aplica un algoritmo a los datos que serán enviados, el cual genera una secuencia de bits y ésta se agrega a dichos datos. Una vez que los datos llegan a su destino, el valor MAC del mensaje garantiza la integridad del mensaje y lo autentica, esto es, si el cálculo del valor MAC no coincide con el valor MAC enviado, el mensaje fue modificado.

  El valor MAC del mensaje garantiza la integridad de dicho mensaje. De esta manera, un código de autenticación de mensajes preserva la integridad de los mensajes enviados a través de un canal inseguro.

- Modification Detection Code (o MDC): El código de detección de modificación es una suma de comprobación de los datos generada utilizando un algoritmo criptográfico, eso es, a los datos que serán enviados se les aplica un cierto algoritmo el cual genera una secuencia de bits y ésta se adiciona a los datos. Una vez que los datos llegan a su destino, si la secuencia de bits generada es la misma, se considera que los datos llegaron a su destino sin modificación alguna.

2.2.4 NO REPUDIO

Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades participantes ha realizado una comunicación. Ofrece protección a un usuario frente a que otro usuario que niegue posteriormente que en realidad se realizó dicha comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. Puede ser de dos tipos:

- Con prueba de origen. Cuando el destinatario tiene prueba del origen de los datos.

- Con prueba de entrega. Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

Los mecanismos de seguridad más empleados para este fin son lo siguientes, siendo la firma digital el más importante y más utilizado.

- Libretas de visitantes: Con base en estos registros se puede constatar la presencia de usuarios y personal en una organización. El nombre de la persona, así como la fecha y hora de su presencia son elementos indispensables para este tipo de mecanismos.

- Bitácora: Registro cronológico de las actividades que ocurren en determinada área de una organización; al igual que en las libretas de visitantes, la fecha y la hora juegan un papel muy importante en el uso de bitácoras.

- Cámaras de video: La evidencia en video siempre es importante cuando se habla de seguridad por lo que las cámaras no deben faltar en la infraestructura de una organización.

- Firmas digitales: Este tipo de mecanismo se basa en el uso de claves y algoritmos de cifrado para proteger información. Se deben conocer las claves necesarias para poder tener acceso a la información lo cual brinda autenticidad y confidencialidad. Este tipo de firma puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido.

- Fotografías: Al igual que el video, las cámaras fotográficas son parte vital de la infraestructura de seguridad en una organización al proveer de evidencia visual a una organización que busca proteger sus recursos.

2.2.5 DISPONIBILIDAD

En este servicio de seguridad se requiere que los recursos del sistema informático estén disponibles para las entidades autorizadas cuando los necesiten. Este servicio mantiene la capacidad de acceder a la información siempre que se requiera.

La no disponibilidad de un sistema o parte de la información en él contenida ocasiona como efecto inmediato una pérdida de tiempo que puede desembocar, por ejemplo, en la pérdida de clientes en una empresa.

Algunos mecanismos de seguridad utilizados para este servicio son:

- UPS (Unit Power Supply): Estos dispositivos son fuentes de energía que se utilizan para que en caso de que ocurra un corte o alguna anomalía en la corriente eléctrica que suministra energía a la organización, los equipos no se vean afectados y no se pierda continuidad en los procesos de la organización, protegiendo, además, el estado físico de los equipos.

- Respaldos: Este tipo de mecanismo funciona para tener copia de toda la información que se considere indispensable en una organización.

- Sistemas distribuidos: Un sistema distribuido se define como una colección de computadoras separadas físicamente y conectadas entre sí por una red de comunicaciones distribuida; estos sistemas son confiables, ya que si un componente del sistema se descompone otro componente es capaz de reemplazarlo, generando tolerancia a fallas.

- Mirrors: Un mirror es un servidor, página WEB o cualquier otro recurso que es espejo de otro, es decir, tiene una copia de la información. Los Mirrors (espejos) facilitan el acceso a la información de aquellos usuarios que se encuentran alejados de la ubicación física del original. Se utilizan para que la carga de páginas o la descarga de archivos sea más rápida al tener un mirror más cerca de un usuario.

2.2.6 CONTROL DE ACCESO

Este servicio requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etcétera) sea controlado y limitado, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.

Se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el usuario está autorizado a comunicar con el receptor o a usar los recursos de comunicación requeridos.

Este control consta generalmente de dos pasos:

- En primer lugar, la autenticación, que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.

- En segundo lugar, procede la cesión de derechos, es decir, la autorización, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etcétera.

Los siguientes son mecanismos de seguridad para este servicio:

- Anuncios: Los señalamientos son parte básica de una organización para que la gente que se encuentre en la organización haga un uso adecuado de las instalaciones, ya sea en ambiente de personal o de usuario/cliente.

- Credenciales: Las credenciales son la forma básica de contar con autenticidad en una organización, ya que cuentan con la información básica para poder identificar a una persona.

- Contraseñas: Una contraseña es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso de la organización.

- Lectores biométricos: Un lector biométrico consiste en la identificación o verificación de la identidad de forma automática de un individuo, empleando sus características biológicas, psicológicas y de conducta, por medio de distintos dispositivos que utilizan diferentes partes del cuerpo humano para realizar una autenticación muy precisa.

Desde una perspectiva combinada de los distintos tipos de servicios de seguridad se pueden identificar cuatro disciplinas o grupos de servicios de seguridad[1]:

I. Gestión de identidades: Permite validar las fuentes y contabilizar la actividad por toda la infraestructura de la organización; permite crear, y modificar identificadores de usuario; posibilita actualizar contraseñas y revalidar usuarios; permite asignar y revocar derechos de usuarios a los recursos; posibilita revisar cuentas, perfiles y derechos de acceso. Aquí se incluyen como disciplinas operacionales la autenticación y el control de acceso Web y como disciplinas administrativas la actualización de contraseñas y el suministro de cuentas de usuario.

II. Gestión de vulnerabilidades: Permite minimizar el acceso a los puntos de ataque, tanto conocidos como desconocidos; posibilita explorar las configuraciones en busca de debilidades y/o evidencias de compromiso de la seguridad antes y después del incidente; permite remediar o mitigar vulnerabilidades; posibilita filtrar el tráfico y entradas canceladas. Aquí se incluyen como disciplinas operacionales los firewalls y sistemas de prevención de intrusiones y como disciplinas administrativas la valoración de vulnerabilidades y la colocación de parches y remedios.

[1] Artículo “Mecanismos de Seguridad” desarrollado dentro del proyecto LEFIS-APTICE: Legal Framework for the Information Society II (financiado por Socrates 2005. European Commission).

III. Gestión de confianza: Permite aplicar controles basados en la valoración de riesgos de datos y aplicaciones; posibilita diseñar procedimientos para que los usuarios hagan un uso aceptable de los recursos y bases técnicas para el buen uso de los mismos; permite cifrar o firmar electrónicamente datos y programas para confidencialidad e integridad; posibilita validar o aplicar el cumplimiento de la política.

IV. Gestión de amenazas: Permite identificar las actividades inapropiadas o maliciosas y reducir la probabilidad de que los sistemas vean comprometida su seguridad o impacto en el uso legítimo de los equipos; posibilita monitorear las actividades y detectar ataques y situaciones en las que la seguridad se vea comprometida; permite responder a eventos sospechosos; posibilita investigar y recuperarse de situaciones en las que se ha visto comprometida la seguridad con éxito. Aquí se incluyen como disciplinas operacionales el monitoreo de datos en busca de fugas, el monitoreo de seguridad con sistemas de detección de intrusiones y los antivirus y como disciplinas administrativas la gestión de eventos de seguridad y la respuesta ante incidentes y el análisis forense.

CAPÍTULO 3

Herramientas de Seguridad Informática

3.1 PANORAMA GENERAL

Actualmente es imprescindible disponer de un adecuado sistema de protección en los sistemas informáticos que asegure desde la privacidad de los datos hasta la seguridad en las transacciones de información. Es por esto que después de haber realizado un análisis de seguridad para el entorno correspondiente, con el cual se identificarán las amenazas y vulnerabilidades, es aconsejable instalar herramientas de seguridad adecuadas.

3.2 HERRAMIENTAS LÓGICAS

Las herramientas lógicas (herramientas de sistema operativo, contrafuegos, escáneres de puertos y vulnerabilidad, IDS, herramientas de análisis y administración, herramientas de cifrado, herramientas para las comunicaciones en red, herramientas forenses, etcétera) hacen referencia a las barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático.

3.2.1 HERRAMIENTAS DEL SISTEMA OPERATIVO

El sistema operativo está formado por el software que permite acceder y realizar las operaciones básicas en una computadora personal o sistema informático en general. Los sistemas operativos más conocidos son: AIX (de IBM), GNU/Linux, HP-UX (de HP), MacOS (Macintosh), Solaris (de SUN Microsystems), las distintas variantes del UNIX de BSD (FreeBSD, OpenBSD), y Windows en sus distintas variantes (de la empresa Microsoft).

En lo que a seguridad se refiere, un sistema operativo puede caracterizarse por:

I. La seguridad en el diseño: hay sistemas operativos que han sido creados con la seguridad como objetivo fundamental de diseño. Éstos serán de entrada más seguros que los demás. En otros sistemas operativos aunque no fuera el objetivo fundamental sí ha podido ser un parámetro importante y por último en otros no se ha considerado más que a posteriori. Es de esperar que sean éstos últimos los que más problemas de seguridad tienen.

   Un sistema más complejo tendrá más errores relacionados con la seguridad en su análisis, diseño y programación. Y desgraciadamente, el número de errores y la dificultad de evaluación no crecen de acuerdo con la complejidad, crecen mucho más rápido.

II. Capacidades de comunicación y configuración: los sistemas operativos modernos ofrecen grandes capacidades de comunicación. Desde el punto

de vista de la seguridad, estas capacidades pueden convertirse en puntos de acceso para posibles atacantes y será necesario protegerlos. El sistema operativo deberá proveer de los mecanismos y herramientas necesarias para llevar a cabo esta tarea de forma suficientemente fiable. Esto incluye ofrecer la capacidad de cerrar toda vía de comunicación que no se use y limitar la que sí se emplee a los casos y usuarios que realmente se deseen permitir.

Desde el punto de vista de seguridad, la manera más segura de tener la configuración del host[2] es inicialmente instalar las herramientas mínimas del sistema operativo, en otras palabras, instalar el corazón del sistema operativo con sólo una cuenta de administrador y un acceso restringido. Posteriormente se agregarán cuentas de usuarios, instalación de aplicaciones, otorgamiento de permisos para dichas aplicaciones, etcétera. Desafortunadamente el proceso de instalación de muchos sistemas operativos, no facilita lo antes mencionado ya que se instalan componentes innecesarios sin permisos, es decir, se instala la configuración por default.

La seguridad de un sistema operativo involucra deshabilitar o borrar servicios innecesarios, librerías o algún otro componente extraño que se instala por default. Por ejemplo el compilador en C como el GCC[3] se instala por default en Linux, pero rara vez esta herramienta es utilizada. Cuando un sistema está comprometido y una utilidad como GCC está habilitada, es fácil para el atacante compilar algún código de ataque o instalar alguna puerta trasera (backdoor)[4] al sistema para el cual le permita acceder en un futuro determinado.

III. Capacidades de auditoría: estas capacidades son las que van a permitir determinar qué elementos acceden a qué partes del sistema en sus distintos niveles (ficheros, dispositivos, elementos de comunicación), etcétera. Los auditores son llamados periódicamente para examinar las transacciones recientes de una organización y para determinar si ha ocurrido actividad fraudulenta.

El registro de auditoría es un registro permanente de acontecimientos de importancia que ocurren en el sistema de computación. Se produce

[2] A una máquina conectada a una red de computadoras y que tiene un nombre de equipo (en inglés, hostname). Es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser una computadora, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etcétera.

[3] GCC es un compilador del lenguaje C, posteriormente se extendió para compilar C++. Este compilador se considera estándar para los sistemas operativos derivados de UNIX. GCC puede realizar tareas como identificar archivos objeto u obtener su tamaño para copiarlos, traducirlos o crear listas, enlazarlos, o quitarles símbolos innecesarios.

[4] Backdoor: Es una secuencia especial dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema. Estas puertas traseras pueden ser perjudiciales ya que permiten al creador del backdoor tener acceso al sistema, hacer lo que desee con él y disponer de ellos libremente.

automáticamente cada vez que ocurren los eventos y es almacenado en un área protegida del sistema. Las auditorías periódicas prestan atención regularmente a problemas de seguridad; las auditorías al azar ayudan a detectar intrusos.

Existen varios mecanismos que pueden usarse para asegurar los archivos, segmentos de memoria, CPU, y otros recursos administrados por el sistema operativo.

Por ejemplo, el direccionamiento de memoria[5] asegura que unos procesos puedan ejecutarse sólo dentro de sus propios espacios de dirección.

La protección hace referencia a los mecanismos para controlar el acceso de programas, procesos, o usuarios a los recursos definidos por un sistema de computación.

El monitoreo de amenazas es una manera de reducir los riesgos de seguridad teniendo rutinas de control en el sistema operativo para permitir o no el acceso a un usuario. Estas rutinas interactúan con los programas de usuario y con los archivos del sistema. De esta manera, cuando un usuario desea realizar una operación con un archivo, las rutinas determinan si se niega o no el acceso y en caso de que el mismo fuera permitido devuelven los resultados del proceso.
Además las rutinas de control permiten detectar los intentos de penetración al sistema y advertir en consecuencia.

Se puede mejorar significativamente la seguridad en los sistemas operativos si se deshabilitan servicios y aplicaciones innecesarias, se limita al acceso a los datos, si se tiene un control de acceso de los usuarios así como los privilegios que tienen e instalar las actualizaciones al sistema operativo.

3.2.2 CORTAFUEGOS O FIREWALLS

Un firewall (o contrafuegos) es un filtro capaz de controlar todas las comunicaciones entrantes y salientes que pasan de una red a otra. Protege a una computadora o una red interna de intentos de acceso no autorizados desde Internet, denegando las transmisiones y vigilando todos los puertos de red.

[5] Direccionamiento de memoria: Ordenamiento o asignación de las direcciones de memoria a los registros.

En la figura 3.1 se muestra un esquema del funcionamiento de un firewall por hardware y por software.

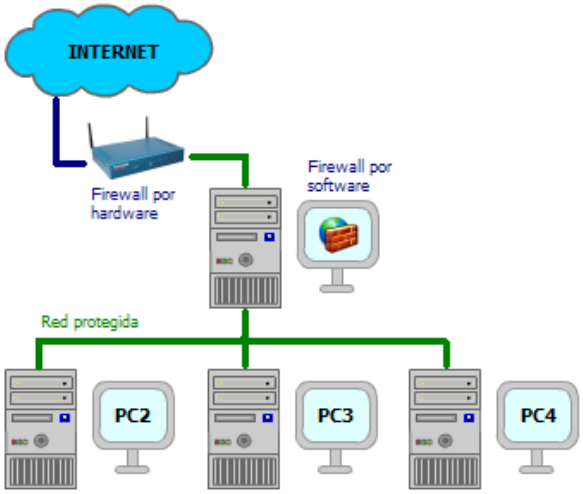


Figura 3.1 Funcionamiento de un Firewall.

Existen dos tipos de Firewall:

- Firewalls de software: Su instalación y actualización es sencilla, pues se trata de una aplicación de seguridad, como lo sería un antivirus; de hecho, muchos antivirus e incluso el propio Windows poseen firewalls para utilizar. Son de bajo costo y es recomendable cuando sólo se utiliza una PC.

  La desventaja de los cortafuegos de software es que protegen solamente a la computadora en el que está instalado y no protegen una red.

- Firewalls de hardware: Los cortafuegos de hardware proporcionan una fuerte protección contra la mayoría de las formas de ataque que vienen del mundo exterior y se pueden comprar como producto independiente o en routers de banda ancha[6].

  Desafortunadamente, luchando contra virus, gusanos y troyanos, un cortafuegos de hardware puede ser menos eficaz que un cortafuegos de software, pues podría no detectar gusanos en correos electrónicos.

[6] Routers de banda ancha: Dispositivos encargados de encaminar y transmitir paquetes de información a una gran velocidad de transmisión entre diferentes redes informáticas.

En la figura 3.2 se observa un firewall de hardware.

Figura 3.2 Firewall por hardware.

3.2.3 ESCÁNERES DE PUERTO Y VULNERABILIDAD

El escáner de puerto y vulnerabilidad es una aplicación que permite realizar una verificación de seguridad en una red mediante el análisis de los puertos abiertos en uno de los equipos o en toda la red.

En general, con este tipo de herramienta es posible efectuar un análisis en una serie o lista de direcciones IP a fin de realizar una verificación completa de una red.

El escáner de vulnerabilidades permite identificar los puertos que están abiertos en un sistema al enviar solicitudes sucesivas a diversos puertos, además de analizar las respuestas para determinar cuáles están activos.

Mediante un análisis exhaustivo de la estructura de los paquetes TCP/IP recibidos, los escáneres de seguridad avanzados pueden identificar, a veces, qué sistema operativo está utilizando el equipo remoto, así como las versiones de las aplicaciones asociadas con los puertos y, cuando sea necesario, recomendar actualizaciones.

3.2.4 SISTEMAS DE DETECCIÓN DE INTRUSOS (O IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa que se usa para detectar accesos no autorizados a una computadora o a una red. La forma en que un IDS detecta las anomalías puede variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a sus recursos.

Un IDS protege a un sistema contra ataques, malos usos y compromisos. Puede también monitorear la actividad de la red, auditar las configuraciones de la red y sistemas por vulnerabilidades, analizar la integridad de los datos entre otros.

Existen varios tipos de IDS, a continuación se mencionan algunos:

- HIDS (Host Intrusion Detection System): este tipo de IDS requiere la implementación de un sistema de detección en cada host individual. Sin importar en qué ambiente de red resida el host, éste estará protegido. Observan una gran cantidad de eventos, de esta manera determinan qué procesos y usuarios se involucran en una determinada acción.

- NIDS o NetIDS (Network Intrusion Detection System): basado en red, filtra los paquetes a través de un dispositivo simple antes de comenzar a enviar a hosts específicos, trabaja a nivel TCP/IP y a nivel de aplicación. Analiza los paquetes capturados buscando patrones que pueden simular algún tipo de ataques. Este tipo de IDS monitorea muchas máquinas dentro de una red ya que analiza y observa en tiempo real todos los paquetes que circulan por un segmento de red aunque éstos no vayan dirigidos a un determinado equipo.

- LFM (Log File Monitors): Este IDS monitorea archivos específicos dentro de una red, buscando un patrón que indique el ataque de un intruso.

3.2.5 HERRAMIENTAS DE ANÁLISIS Y ADMINISTRACIÓN

Hoy en día las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante. Las redes, cada vez, soportan aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez más importante y de carácter pro-activo para evitar problemas.

Una de las herramientas más importantes en el análisis de una red es Nmap (Network Mapper). Esta herramienta envía paquetes TCP y UDP a un grupo de máquinas de una red (determinada por la dirección de la red y una máscara) analizando posteriormente las respuestas. Según la velocidad de los paquetes TCP recibidos, puede determinar el sistema operativo remoto para cada máquina analizada.

Dentro de las herramientas para la administración de una red se encuentra el protocolo SNMP (Simple Network Manager Protocol), el cual es un protocolo de nivel de aplicación que proporciona una estructura de mensajes para el intercambio de información entre administradores y agentes SNMP. Proporciona un estandarizado entorno de trabajo, un lenguaje común empleado para el monitoreo y la administración del dispositivo en red.

El protocolo SNMP está conformado por tres elementos, los cuales son:

- Administrador SNMP: Controla la actividad de los componentes de la red mediante SNMP.

- Agente SNMP: Es un software que se encuentra dentro del dispositivo administrado el cual contiene variables de la MIB cuyos valores pueden ser solicitados o modificados por el administrador SNMP.

- MIB (Management Information Base): Es un tipo de base de datos la cual contiene información de todos los dispositivos gestionados en una red de comunicaciones.

El protocolo SNMP funciona de acuerdo con el modelo cliente/servidor, donde el proceso servidor se ejecuta en los agentes y permanece escuchando las peticiones por parte del administrador SNMP.

3.2.6 HERRAMIENTAS DE CIFRADO

El cifrado de datos garantiza que la información sea ilegible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.

Existen tres tipos de cifrado:

- Sistema de cifrado simétrico: Son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por tal motivo se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave, además de que dicha clave sea muy difícil de adivinar.

  Hoy por hoy se están utilizando ya claves de 128 bits que aumentan el número de claves posibles (2 elevado a 128).

  El principal problema con los sistemas de cifrado simétrico es el número de claves que se necesitan. Si se tiene un número n de personas que necesitan comunicarse entre sí, se necesitan n/2 claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

- Sistema de cifrado asimétrico o de clave pública: Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a

cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario puede descifrarse, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

- Sistema de cifrado híbridos: Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente, por lo que si un atacante descubre la clave simétrica, sólo le valdría para ese mensaje y no para los restantes.

3.2.7 HERRAMIENTAS PARA LAS COMUNICACIONES EN RED

La planificación de la seguridad en el diseño de la red es de suma importancia pues de esto depende el buen desempeño de la red y evita trabajo posterior y pérdida de datos y posibles daños a la red.

Hoy en día la seguridad en las redes se ha convertido en un factor importante en el diseño e implementación de las redes. El administrador de la red debe estar constantemente implementando medidas de seguridad en la red con el fin de tener una red confiable y estable. El trabajo del administrador deberá incluir la administración de usuarios, tomar en cuenta el uso de cortafuegos que permita administrar el acceso de usuarios de otras redes así como monitorear las actividades de los usuarios de la red, esto es, el administrador se da cuenta de los accesos no autorizados por parte de los usuarios y debe tomar las medidas que faciliten incrementar la seguridad. Las bitácoras son de gran utilidad para aplicar auditorías a la red.

La seguridad basada en la autenticación de usuario es la más usada, permite administrar y asignar derechos a los usuarios de la red. Permitiendo o denegando los accesos a los recursos a través de una base de datos en el servidor.
Algunos puntos que se deben tomar en cuenta son:

- Accesos no autorizados.
- Daño intencionado y no intencionado.
- Uso indebido de información (robo de información).

El nivel de seguridad de la red dependerá de su tamaño e importancia de la información.

Seguridad en redes inalámbricas

Debido a que las redes inalámbricas utilizan como medio físico de transmisión el aire, el factor de seguridad es crítico.

Uno de los puntos débiles (debe considerarse el gran punto débil) es el hecho de no poder controlar el área que la señal de la red cubre, por esto es posible que la señal exceda el perímetro del edificio y alguien desde afuera pueda visualizar la red y esto es sin lugar a dudas una oportunidad para el posible atacante.

La seguridad de este tipo de redes se ha basado en la implantación de la autenticación del punto de acceso y los clientes con tarjetas inalámbricas permitiendo o denegando los accesos a los recursos de la red.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones para enviar datos a través de Internet deben considerarse también para las redes inalámbricas.

Los mecanismos de seguridad para las WLAN son:

I. WEP (Wired Equivalent Privacy): Es el sistema de cifrado incluido en el estándar IEEE 802.11[7] como protocolo para redes Wireless[8] que permite cifrar la información que se transmite. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

   WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca el aumento de mantenimiento por parte del administrador de la red, lo que conlleva en la mayoría de ocasiones, que la clave se cambie poco o nunca.

[7] El estándar IEEE 802.11 o Wi-Fi de IEEE especifica sus normas de funcionamiento en una WLAN, provee velocidades de hasta 2Mbps.

[8] La comunicación inalámbrica (inglés wireless, sin cables) no se utiliza un medio de propagación físico alguno, esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión.

WEP no incluye autenticación de usuarios. Lo más que incluye es la autenticación de estaciones (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). A pesar de los defectos de este sistema de cifrado, el protocolo WEP sigue siendo muy popular y posiblemente el más utilizado. Esto es debido a que WEP es fácil de configurar y cualquier sistema con el estándar 802.11 lo soporta.

II. WPA (Wi-Fi Protected Access): Es un sistema para proteger las redes inalámbricas (Wi-Fi[9]); creado para corregir las deficiencias del sistema previo WEP.

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.

WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse. Al incrementar el tamaño de las claves, el número de claves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil.

Una de las ventajas de los sistemas WAP es que se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

III. WPA2 (Wi-Fi Protected Access 2): Creado para corregir las vulnerabilidades detectadas en WPA. Incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), por este motivo requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

Seguridad en redes LAN (del inglés Local Area Network)

Una red de área local es la interconexión de varias computadoras y periféricos para compartir recursos e intercambiar datos y aplicaciones. Su extensión está limitada físicamente a un edificio o a un entorno de hasta 200 metros.

Una red de área local permite compartir bases de datos, programas y periféricos como puede ser un módem, una impresora, etcétera; poniendo a disposición otros

[9] Wi-Fi: Es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables.

medios de comunicación como pueden ser el correo electrónico y el chat. Permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.
Para mantener la seguridad en redes LAN es importante limitar el acceso a los equipos sólo a usuarios permitidos. Así mismo se hace uso de firewalls y sistemas detectores de intrusos para mantener la red segura.

Es importante considerar además la forma geométrica en que están distribuidos los equipos de una red, cuyo objetivo es conseguir la forma más económica y eficaz para facilitar la funcionalidad del sistema, evitar tiempos de espera y hacerla más segura.

Así mismo se deben considerar los medios de transmisión los cuales reciben el nombre de guiados o terrestres:

- Par trenzado: Cable en cuya conexión dos conductores son entrelazados para cancelar las interferencias electromagnéticas (IEM) de fuentes externas y la diafonía de los cables adyacentes.

  Velocidad de operación de 10Mbps, distancia máxima de 100m. Emplea la norma 568a y 568b[10].

- Cable coaxial: Cable utilizado para transportar señales eléctricas de alta frecuencia. Velocidad de operación de 10Mbps. Longitud máxima 185m y una mínima de 0.5m entre nodos.

- Fibra óptica: es un medio de transmisión el cual maneja luz (en lugar de corriente o voltajes eléctricos). Tiene una velocidad de operación de 10Mbps, es inmune al ruido electromagnético y posee dimensión y pequeño peso.

  Todos estos factores anteriormente mencionados son indispensables para mantener la seguridad en una red LAN.

Es indispensable que el diseño y la implementación de una red estén bajo las normas más actuales de seguridad, ya que esto traerá consigo una mayor robustez en cuanto a protección de la información y la organización a su vez, ganará prestigio si se encuentra la vanguardia en cuanto a normas de seguridad.

[10] EIA/TIA 568ª y EIA/TIA 568 b: Estas normas especifican un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante. Permiten la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad.

3.2.8 HERRAMIENTAS FORENSES

Se denomina análisis forense al proceso de analizar una copia completa de un sistema que ha sufrido una intrusión o ataque.

El análisis forense permite obtener la mayor cantidad posible de información sobre:

- El método utilizado por el atacante para introducirse en el sistema.
- Las actividades ilícitas realizadas por el intruso en el sistema.
- El alcance y las implicaciones de dichas actividades.
- Las puertas traseras instaladas por el intruso.

La realización de un análisis forense logra, entre otras cosas, una recuperación del incidente de una manera más segura evitando en la medida de lo posible que se repita la misma situación en cualquiera de las máquinas.

Un buen análisis forense debe dar respuestas a varias cuestiones, entre las que se encuentran las siguientes:

a) ¿En que fecha exacta se ha realizado la intrusión o cambio?

b) ¿Quién realizó la intrusión?

c) ¿Cómo entró en el sistema?

d) ¿Qué daños ha producido en el sistema?

Estas herramientas sólo funcionan si se usan con privilegios de administrador.

3.3 HERRAMIENTAS FÍSICAS

La seguridad física implica la aplicación de procedimientos de control y barreras físicas como medidas de precaución y control ante amenazas que puedan afectar los recursos de una organización. Estos procedimientos de control se realizan por medio de barreras físicas, materiales que permiten mantener el control y el resguardo en los recursos.

3.3.1 SENSORES BIOMÉTRICOS[11]

Históricamente, la identificación personal se ha basado en posesiones especiales (llaves, tarjetas) o en conocimientos secretos (palabras claves, Números de Identificación Personal), todos éstos con aspectos en común, son únicos, y se emplean para verificar la identidad de su portador. Ahora bien, el ser humano posee características que lo hacen único, como las huellas dactilares, la voz, el rostro, e incluso el iris del ojo. Entonces por analogía, el cuerpo humano puede funcionar como un tipo de clave. Esto es la esencia del mundo de la biometría, la cual consiste en la identificación o verificación de la identidad de forma automática de un individuo, empleando sus características biológicas, psicológicas y de conducta.

Un sistema biométrico por definición, es un sistema automático capaz de:

a) Obtener la muestra biométrica del usuario final.

b) Extraer los datos de la muestra.

c) Comparar los datos obtenidos con los existentes en la base de datos.

d) Decidir la correspondencia de datos.

e) Indicar el resultado de la verificación.

Existen sistemas que procesan las siguientes variables biométricas:

- Reconocimiento de rostro.
- Reconocimiento de la voz.
- Patrón del iris.
- Huellas dactilares.
- Mapa de la retina.
- Olor corporal.
- Forma del oído.
- Forma de la mano.
- Geometría de los dedos.

[11] Para información detallada léase el apéndice B

- Forma de la cabeza.
- Mapa de venas de la mano.

De todos los sistemas mencionados anteriormente, los más comunes comercialmente son:

- Reconocimiento de huellas dactilares.
- Patrón del iris.
- Reconocimiento de voz.

Entre todas las técnicas biométricas la identificación basada en las huellas dactilares es el método más viejo. Una huella está formada por una serie de crestas y surcos localizados en la superficie del dedo. La singularidad de una huella puede ser determinada por dos tipos de patrones: el patrón de crestas y surcos, así como el de detalles.

Patrón de iris[12]

El iris es un órgano interno del ojo, localizado por detrás de la cornea y del humor acuoso, pero enfrente de los lentes.

Una propiedad que el iris comparte con las huellas dactilares es la morfología aleatoria de su estructura. No existe alteración genética en la expresión de este órgano más allá de su forma anatómica, fisiología, color y apariencia general. La textura del iris por sí misma es estocástica o posiblemente caótica.

Ventajas prácticas adicionales sobre las huellas dactilares:

- La facilidad de registrar su imagen a cierta distancia, sin la necesidad de contacto físico o intrusivo y quizás discretamente.
- Estable y sin cambio durante el periodo de vida del sujeto.

Reconocimiento de voz

En un sistema para el reconocimiento de voz, se emplea la biometría física y de conducta con el objetivo de analizar patrones de habla e identificar al interlocutor. Para llevar a cabo esta tarea, el patrón creado previamente por el interlocutor, debe ser digitalizado y mantenido en una base de datos que generalmente es una cinta digital de audio.

[12] Para información detallada léase el apéndice B

3.3.2 BITÁCORAS

Una bitácora es el documento donde se registran los acontecimientos e incidentes de un día, el registro es cronológico, sucesivo. En el mundo computacional, un sistema, un autor o un conjunto de ellos generan mensajes de una manera cronológica, sucesiva, sobre temas concretos. La principal singularidad de la bitácora es la sencillez (además de su bajo costo).

Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera:

- Fecha y hora: Indispensables para la investigación al buscar las causas y causantes de algún incidente en la organización.
- Direcciones IP origen y destino: Parte importante de un análisis que busque responsables en un incidente; estas direcciones indican la parte emisora y receptora en una comunicación.
- Dirección IP que genera la bitácora: Aporta la dirección del equipo en donde se genera la bitácora.
- Usuarios: Tener un registro de los usuarios en la bitácora es necesario al tener en marcha una investigación en búsqueda de personas involucradas en algún incidente.
- Errores: La cronología de los errores es importante para poder detectar causas de un incidente.

En el campo de la seguridad informática, las bitácoras son útiles para la recuperación ante incidentes de seguridad ya que aportan información útil para la detección de comportamiento inusual en un sistema, así como evidencia legal para resolver incidentes que ocurran en la organización.

Los eventos que se analizan en una bitácora que se utiliza como herramienta física de seguridad informática deben tener relación con:

- El sistema que se utiliza: Es importante que se conozca el sistema que se utiliza para saber cuáles son sus vulnerabilidades.
- Correo: Es parte importante al momento de investigar un incidente ya que constituye uno de los medios por los cuales se puede ser atacado.

- Ruteadores, switches, firewalls, IDS´s: El tráfico que fluye en estos dispositivos y herramientas es indispensable en un análisis que busque responsables y causas en un incidente.

- Web: El registro del tráfico de web que ocurre en la organización también es importante debido a que es un puente entre una amenaza y la organización.

Las bitácoras contienen información crítica del sistema en uso, es por ello que deben ser analizadas periódicamente y éstas necesitan tener acceso a todo dispositivo que se encuentre activo en la organización.

3.3.3 TARJETAS

Como herramienta de seguridad física, existen distintos tipos de tarjetas que van desde un diseño muy simple (con un nivel bajo de seguridad), hasta un diseño complejo que permite un grado robusto de seguridad.

Las tarjetas más simples contienen la información más básica de un usuario (como el nombre, una fotografía, sexo, departamento, etcétera) pero la protección que ofrecen para dicha información es muy baja ya que no cuentan con ningún mecanismo en específico para este propósito y sólo funcionan como un simple control de acceso.

Las tarjetas más complejas utilizadas como herramienta de seguridad son tarjetas de plástico similares en tamaño y otros estándares físicos a las tarjetas de crédito que llevan estampadas un circuito integrado. Este circuito puede ser una memoria o contener un microprocesador con sistema operativo que realice tareas como:

- Almacenar.

- Cifrar información.

- Leer y escribir datos.

Como mecanismo de control de acceso las tarjetas hacen que los datos personales y de negocios sólo sean accesibles a los usuarios apropiados.
Las tarjetas dependen de tres zonas fundamentales:

I. Zona Abierta: Contiene información que no es confidencial. (el nombre del portador y su dirección).

II. Zona de Trabajo: Contiene información confidencial. Por ejemplo, información bancaria).

III. Zonas Secretas: La información es totalmente confidencial. El contenido de estas zonas no es totalmente disponible para el portador de la tarjeta, ni tiene por qué conocerla la entidad que la emite, ni siquiera quien la fabrica.

Las tarjetas se activan al introducirlas en un lector de tarjetas. Un contacto metálico, o incluso una lectura láser, permiten la transferencia de información entre el lector y la tarjeta.

Los tipos más importantes de tarjetas son:

- Tarjeta inteligente de contacto: Estas tarjetas son las que necesitan ser insertadas en una terminal con lector inteligente para que por medio de contactos pueda ser leída, existen dos tipos de tarjeta inteligente de contacto: las sincrónicas y las asincrónicas.

- Tarjetas inteligentes sincrónicas: Son tarjetas con sólo memoria y la presentación de esta tarjeta inteligente y su utilización se concentra principalmente en tarjetas prepagadas para hacer llamadas telefónicas.

- Tarjetas asincrónicas: Son tarjetas inteligentes con microprocesador, ésta es la verdadera tarjeta inteligente, tiene el mismo tamaño y grosor de una tarjeta de crédito, pueden tener una cinta magnética en la parte posterior. Dentro del plástico se encuentra un elemento electrónico junto con la memoria RAM, ROM y EEPROM en el mismo chip.

Como cualquier herramienta física de seguridad, las tarjetas presentan algunas ventajas y desventajas, las cuales son importantes señalar.

Ventajas:

- Facilidad para implementar control de acceso

- Altos niveles de seguridad si se trata de tarjetas con circuito integrado.

- Reducción del fraude tratándose de tarjetas con circuito integrado.

- Fácil manejo de información.

- Facilidad de usos sin necesidad de conexiones en línea o vía telefónica.

- Comodidad para el usuario.

Desventajas:

- Molestias al recuperar información de una tarjeta robada.

- Por su tamaño se puede extraviar fácilmente.
- Dependencia de la energía eléctrica para su utilización (en el caso de tarjetas con circuito integrado).
- Vulnerables a los fluidos.

3.3.4 DETECTORES DE METALES

Un detector de metales es el instrumento que mediante una serie de impulsos electromagnéticos es capaz de detectar objetos metálicos magnéticos y ferromagnéticos.

Los detectores de metales no considerados como portátiles (seguridad personal y antiminas), se componen de arcos o túneles de detección conocidos como "Cabezales de Detección de Metales".

Estos túneles que generan un campo electromagnético en su interior, pueden ser cuadrados, rectangulares o incluso circulares. Los túneles circulares se utilizan para inspeccionar el paso de los productos a través de tuberías, mientras que los rectangulares se utilizan en las cintas de transporte.

3.3.5 CHAPAS

Se denomina chapa a una lámina delgada de metal que se utiliza para resguardar construcciones. Las chapas de seguridad son parte fundamental de una organización en cuanto a su seguridad física, ya que son una de las primeras barreras que un atacante se encuentra al intentar dañar los activos de una organización.

Existen diversos tipos de cerraduras de seguridad, todas con un nivel distinto de complejidad y con características diferentes dependiendo de las necesidades de una organización.

3.3.6 TECLADOS[13]

Existen ciertos métodos para poder realizar un ataque a una organización por medio de sus teclados, siendo uno de los más usados, el del keylogger. Como su nombre lo indica un keylogger es un programa que registra y graba la pulsación de

[13] Tomado del artículo: Keyloggers, Autor: Lic. Cristian F. Borghello con la colaboración de Douglas Schillaci; http://www.segu-info.com.ar

teclas (y algunos también de clicks del mouse). La información recolectada es utilizada posteriormente por la persona que lo instaló. Actualmente existen dispositivos de hardware o aplicaciones (software) que realizan estas tareas.

Los keyloggers físicos son pequeños dispositivos que se instalan entre la computadora y el teclado. Son difíciles de identificar para un usuario inexperto pero si se presta atención es posible reconocerlos a simple vista. Tienen distintas capacidades de almacenamiento, se compran en cualquier casa especializada y generalmente son instalados por empresas que desean controlar a ciertos empleados, sin embargo, también pueden ser utilizados para propósitos maliciosos al intentar obtener información privada por medio de ellos.

Existen 3 tipos de keyloggers hardware:

- Adaptadores en línea que se intercalan en la conexión del teclado, tienen la ventaja de poder ser instalados inmediatamente. Se detectan fácilmente con una revisión visual detallada.

- Dispositivos que se pueden instalar dentro de los teclados estándares, requiere de habilidad para soldar y de tener acceso al teclado que se modificará. No son detectables a menos que se abra el cuerpo del teclado.

- Teclados reales que contienen el keylogger ya integrado. Son virtualmente imperceptibles, a menos que se les busque específicamente.

Con respecto a las keyloggers por software, actualmente son los más comunes, muy utilizados por el malware orientado a robar datos confidenciales o privados del usuario. La información obtenida es todo lo que el usuario ingrese en su teclado como por ejemplo documentos, nombres de usuarios, contraseñas, números de tarjetas, etcétera.

Existen varios tipos de keyloggers, siendo los más importantes:

- Basado en kernel (núcleo): Este método es el más difícil de escribir, y combatir. Tales keyloggers residen en el nivel del núcleo del sistema operativo y son así prácticamente invisibles. Derriban el núcleo del sistema operativo y tienen casi siempre el acceso autorizado al hardware.

- Enganchados: Tales keyloggers enganchan el teclado con las funciones proporcionadas por el sistema operativo. El sistema operativo los activa en cualquier momento en que se presiona una tecla y realiza el registro.

Para contrarrestar este tipo de software malicioso es necesario utilizar firewalls, antyspyware (software utilizado para identificar y eliminar programas maliciosos) e

incluso software anty-keylogger. En lo que respecta a los keyloggers de tipo hardware es necesario realizar revisiones visuales detalladas de los equipos.

Es importante ser consciente que los keyloggers son una herramienta que, como tal, puede utilizarse con fines benéficos pero también dañinos y delictivos como lamentablemente ocurre.

Además de los keyloggers, existen otras formas con las cuales se puede consumar un ataque en una organización, siendo el personal el responsable de crear inconscientemente vulnerabilidades en la infraestructura de la organización. Esto se debe a que algunas personas acostumbran tener escritas sus contraseñas en información importante y confidencial en distintos post-it, los cuales están a la vista de toda persona, ya que generalmente se colocan en el CPU y en los teclados de los equipos. Este tipo de acciones debe ser totalmente prohibida en una organización ya que su seguridad comienza en el personal que labora sus instalaciones.

3.3.7 FEA (FIRMA ELECTRÓNICA AVANZADA)

La FEA es una aplicación de la criptografía asimétrica, en específico del sistema criptográfico de clave pública RSA (siglas derivadas de las iniciales de los apellidos de los autores Ronald Rivest, Adi Shamir y Len Adleman, 1977,) el sistema de criptografía asimétrico más conocido y utilizado.

Se basa en el uso de un juego de clave o llaves, un par de números matemáticamente relacionados, uno para la pública y otro para la privada. Un programa de cómputo los produce y se los proporciona al solicitante, quien puede dar a conocer la primera y debe mantener en secreto la segunda.

Cada clave es la función inversa de la otra, es decir, lo que una clave hace sólo la otra clave puede deshacerlo. Así, para enviar un mensaje privado, el emisor lo cifra (cierra) con la clave pública del receptor y sólo el receptor puede descifrarlo (abrirlo) con su propia clave privada, que nadie más conoce.

Las claves del sistema RSA pueden ser empleadas en ambas direcciones, de tal manera que el emisor puede cifra datos utilizando su clave privada, los cuales sólo podrán ser descifrarlo con su clave pública que comparte con él o los receptores.
Técnicamente, no es posible obtener la clave privada a partir de la pública, aun utilizando la mejor computadora.

De esta forma, la información cifrada con este sistema garantiza la confidencialidad y autenticación.

La Firma Electrónica Avanzada (FEA), además de confidencialidad y autenticación, asegura la integridad del documento (el contenido no puede ser alterado) y el no repudio del mismo (innegable autoría).

La FEA utiliza la función hash para garantizar lo anterior. El hash es una operación matemática que asocia un texto de extensión variable a un número de longitud fija (entre 128 o160 bits) que se llama resumen. Si el documento sufre alguna alteración o modificación, por mínima que sea, el hash cambia, reflejando que el documento ya no es el mismo.

Se asigna un hash para cada documento. Las funciones hash no cifran, sólo comprimen los textos para que el receptor pueda comprobar la integridad del mismo rápidamente. Al aplicar la firma digital, se cifra sólo la función hash y no todo el documento. De esta forma el proceso de descifrado toma menos tiempo.

CAPÍTULO 4

ANÁLISIS DE RIESGO

4.1 DEFINICIÓN

Un análisis de riesgo es un proceso por el cual se identifican las amenazas y vulnerabilidades de una organización con el fin de generar controles que minimicen los efectos de los riesgos. Todo esto siguiendo un estándar internacional de seguridad informática como el ISO/IEC 17799[14].

En la elaboración de un análisis de riesgo es importante conocer el significado de la siguiente terminología:

- Riesgo: Posibilidad de sufrir una pérdida o un daño.

- Activo: Es todo aquello que tiene un valor para la organización, pueden ser datos, infraestructura, hardware, software, personal y su experiencia, información, servicios, etcétera.

- Controles: Mecanismos de protección así como los protocolos que permiten el cumplimiento de las políticas de seguridad en la organización. Por lo general, existen cuatro tipos de controles:

  I. Los disuasorios son controles destinados a reducir la probabilidad de un ataque deliberado.

  II. Los preventivos son controles que protegen de una vulnerabilidad intentando que los ataques sean fallidos o que produzcan el menor impacto posible.

  III. Los correctivos son controles destinados a reducir el efecto de un ataque.

  IV. Los detectores son controles programados para descubrir y desencadenar ataques preventivos o correctivos.

- Vulnerabilidades: Elementos que hacen a un sistema más propenso al ataque de una amenaza o aquellas situaciones en las que es más probable que un ataque tenga cierto éxito e impacto en los procesos de negocio de la organización. Son las debilidades existentes.

- Amenazas: Se trata del conjunto de cosas que pueden “salir mal” o las acciones que pueden “atacar” la información de la entidad. Es algo que puede suceder o existir, pero aún no existe.

[14]Estándar para la seguridad de la información, proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información, posteriormente renombrado como ISO 27002.

- Clasificación de los riegos: En esta clasificación se identifican las fuentes de riesgo existentes y con qué frecuencia eventos no deseados pueden ocurrir así como la magnitud de sus consecuencias.

  En la tabla 4.1 se muestra un ejemplo de la clasificación de los riesgos.

RIESGO	CONSECUENCIA	PROBABILIDAD
Muy alto	Catastróficos	Certeza
Alto	Mayores	Probablemente
Moderado	Moderados	Moderado
Bajo	Menores Insignificantes	Improbable Raro

Tabla 4.1 Ejemplo de una escala de riesgo, consecuencias, así como probabilidad de ocurrencia.

- Riesgo residual: Es el nivel de riesgo que resulta tras considerar las medidas necesarias, niveles de vulnerabilidad y amenazas relacionadas.

El objetivo de un análisis de riesgo es tener la capacidad de:

- Evaluar y manejar los riesgos de seguridad.
- Tomar las mejores decisiones en seguridad informática.
- Enfocar los esfuerzos en la protección de los activos.
- Asegurar la continuidad operacional de la organización.
- Saber manejar las amenazas y riesgos críticos.
- Mantener una estrategia de protección y de reducción de riesgos.
- Justificar una mejora continua de la seguridad informática.

Lo anteriormente mencionado se ilustra en la figura 4.1 la cuál contiene los elementos de un análisis de riegos.

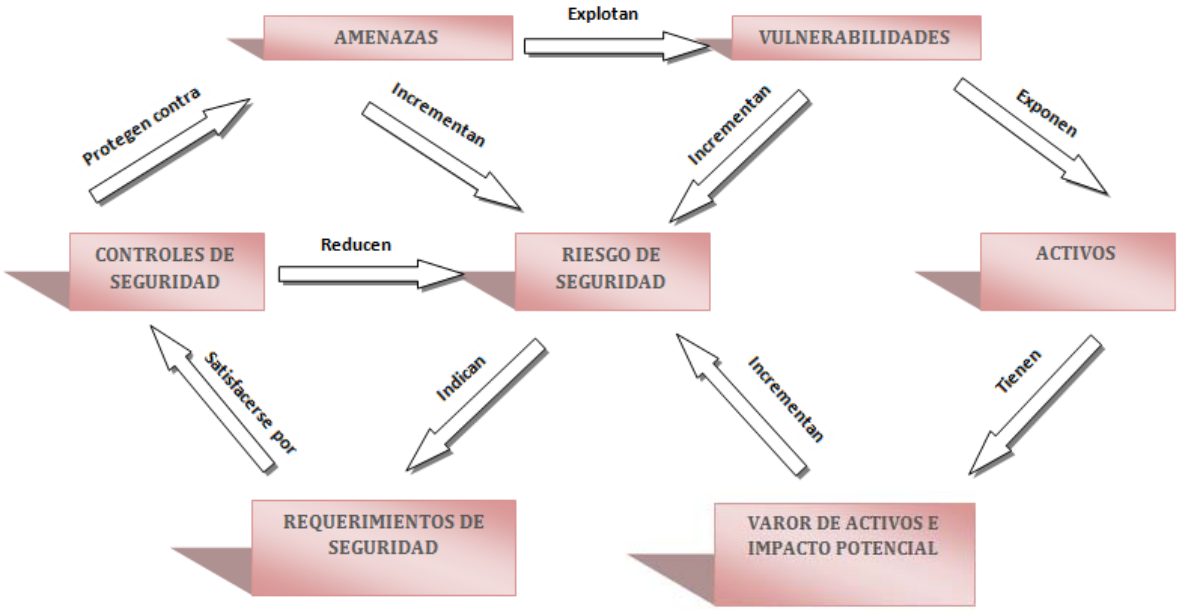


Figura 4.1 Relación de riesgos

El análisis de riesgo es un proceso cíclico y continuo que involucra al área de tecnologías de la información y a la administración.

El proceso involucra (Figura 4.2):

a) Identificación de riegos: Es el proceso de comprender qué eventos potencialmente podrían dañar o mejorar a un proyecto en particular. Se cuenta con varias herramientas y técnicas. Las más utilizadas son la tormenta de ideas, las entrevistas, el análisis causa - efecto, y el análisis FODA (Fortalezas, Debilidades, Oportunidades, y Amenazas).

b) Analizar: Hacer uso sistemático de la información de tal forma que se identifican las fuentes y así determinar qué tan seguido los eventos no deseados pueden ocurrir o no y cuál es la magnitud de sus consecuencias.

c) Planear: Después que una organización identifica y cuantifica los riesgos, se planea una apropiada estrategia para poder enfrentarlos.

b) Implementar: Se realiza la implementación de las medidas de seguridad con la finalidad de proporcionar un nivel de seguridad razonable.

c) Monitoreo y control de riegos: Involucra la ejecución de los procesos de la administración de riesgo para responder a los eventos riesgosos.

Ejecutar los procesos de la administración de riesgos significa asegurar que el reconocimiento de los riesgos es una actividad permanente ejecutada por todos los miembros del equipo a lo largo de la vida del proyecto.

Figura 4.2 Proceso de un análisis de riesgo

Es importante decir que los resultados de un análisis de riesgo proveen información que facilita y justifica la toma de decisiones en relación a la seguridad informática.

4.2 TIPOS

Un riesgo es un evento, el cual es incierto y tiene un impacto negativo.

Existen dos tipos de análisis de riesgo, cuantitativo o cualitativo, los cuales permiten evaluar los riesgos. Esto involucra una estimación de incertidumbre del riesgo y su impacto.

a) Enfoque cuantitativo de análisis de riesgos

Este enfoque emplea dos elementos fundamentales, la probabilidad de que se produzca un hecho y la probable pérdida en caso de que ocurra el hecho citado.

Se basa en dos parámetros fundamentales:

I. La probabilidad de que un suceso ocurra.

II. Estimación del costo o las pérdidas en caso de que así sea.

El producto de ambos términos es lo que se denomina costo anual estimado (EAC, Estimated Annual Cost), y teóricamente es posible conocer el riesgo de cualquier evento (el EAC incluir en el glosario) y tomar decisiones en función de estos datos.

La desventaja de este tipo de análisis de riesgos está asociada con la inexactitud y falta de fiabilidad de los datos. Los datos asociados a las probabilidades estimadas, por lo general bajo el criterio interno de la empresa, en pocas ocasiones suelen ser precisos y pueden, en algunos casos, estar basados en la propia autocomplacencia de los dueños de los procesos de negocio.

b) Enfoque cualitativo de análisis de riesgos

Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos o correctivos).

Con estos cuatro elementos se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

Éste es el enfoque más utilizado para el análisis de riesgos. En este caso, la probabilidad no es necesaria y tan sólo es utilizado como factor de cálculo la pérdida potencial estimada.

Las principales técnicas para el análisis cuantitativo exigen la recolección de datos y valor de los activos.

4.3 PASOS DEL ANÁLISIS DE RIESGO

En la realización de un análisis de riesgo efectuado a alguna organización se debe determinar:

- El nivel actual de riesgo.

- Anticiparse a sus consecuencias y determinar su impacto en las funciones críticas de la organización.
- Disminuir los tiempos y costos.
- Cómo mejorar los resultados de la respuesta.

La planeación de un análisis de riesgo empieza con:

- Construir el perfil de las amenazas basado en los activos.
- Identificar los activos de la organización.
- Identificar las amenazas a los activos.
- Conocer las prácticas actuales de seguridad.
- Identificar las vulnerabilidades organizacionales.
- Recursos humanos, recursos técnicos, etcétera.
- Identificar los requerimientos de seguridad de la organización.

Es por esto que el análisis de riesgo requiere ocho pasos básicos. Estos pasos permiten conocer los riesgos puros (en los que sólo se puede perder); los riesgos del negocio (dinámicos o especulativos), en los que se puede ganar o perder; la máxima pérdida posible si el bien es destruido por el riesgo; la máxima pérdida probable y la expectativa de pérdida anual también brinda los elementos de juicio para saber qué hacer con los principales riesgos.

Conociendo los principales riesgos, se puede optar por eliminarlos, reducirlos, compartirlos, transferirlos o asumirlos.

4.3.1 IDENTIFICACIÓN Y EVALUACIÓN DE ACTIVOS

En este primer paso se identifican los activos que se protegerán y se determina cuál es la importancia para la organización. Deducir la importancia que tiene los activos en la organización implica el conocer los procesos en los que están envueltos y así saber cómo son afectados los procesos de la organización.

Para conocer los activos de la organización se realizan entrevistas al personal, administradores y autoridades de la organización que contribuyan a la recolección de datos que permita identificar los recursos del sistema, al mismo tiempo, estas entrevistas deben arrojar información que ayude a concluir cuál es la importancia

de los activos identificados en ellas. Además, se realizan inspecciones visuales para confirmar y seguir identificando activos en la organización.

Debemos identificar todos los recursos cuya integridad pueda ser amenazada de cualquier forma; por ejemplo, los siguientes:

- Hardware: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers, etcétera.

- Software: Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación, etcétera.

- Información: En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos, impresos, etcétera.

- Personas: Usuarios, operadores, personal en general de la organización.

- Accesorios: Papel, cintas, tóners, etcétera.

Para poder determinar la importancia de los activos identificados, debe tomarse en cuenta el costo de los recursos e información que se busca proteger y su papel en los procesos de la organización, es decir, se debe determinar qué tanto afectan los activos identificados en los procesos y el manejo de la organización.

Es difícil generar estos aspectos intangibles de los recursos, ya que es algo que va a depender de cada organización, su funcionamiento, sus normas, sin embargo, se deben tener en cuenta algunos aspectos comunes: privacidad de los usuarios, imagen pública de la organización, reputación, satisfacción del personal y de los clientes, capacidad de continuar con los procesos en la organización ante una falla.

4.3.2 IDENTIFICAR LAS AMENAZAS CORRESPONDIENTES

De acuerdo con cada organización y su lugar geográfico se definen las amenazas que pueden afectar a los activos.

Después de realizar la identificación de las amenazas, se determinan las pérdidas que se presentarían si dichas amenazas se concretan. Además de estimar la frecuencia de ocurrencia de las amenazas, es decir, qué tan seguido se podrían presentar en la organización.

Algo importante al analizar las amenazas a las que se enfrentan los sistemas, es analizar los potenciales tipos de atacantes que pueden intentar violar la seguridad. Es algo normal que al hablar de atacantes la mayoría piense en crackers, en

piratas informáticos mal llamados hackers. No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

No siempre se debe contemplar a las amenazas como actos intencionados contra un sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación.

4.3.3 IDENTIFICAR/DESCUBRIR VULNERABILIDADES

El priorizar los riesgos en la organización es el objetivo de este paso; el nivel de riesgo se determina analizando la relación entre las amenazas y las vulnerabilidades. Un riesgo existe cuando una amenaza tiene una vulnerabilidad correspondiente.

Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en la organización.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse con base en el nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que costaría recuperarse de un daño en él o de su pérdida total.

4.3.4 DETERMINAR EL IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

Cuando una amenaza explota una vulnerabilidad, los activos sufren un daño y a la vez se causa un impacto en los procesos de una organización. Las pérdidas y los daños son catalogados en cuatro áreas de impacto:

- Revelación: En esta área se catalogan los daños que se presentan cuando la información es procesada y se pierde la confidencialidad.

- Modificación: El ataque cambia el estado original de algún archivo.

- Destrucción: El activo es atacado produciendo su pérdida total.

- Denegación del servicio: En esta área se catalogan las pérdidas producidas por la pérdida temporal de los servicios.

En una organización, existen áreas de alta vulnerabilidad que no tienen consecuencias si no se presentan amenazas.

4.3.5 CONTROLES EN EL LUGAR

Control se refiere a los protocolos y mecanismos de protección que permiten que las estrategias de seguridad en una organización se cumplan.

En este paso del análisis se identifican los controles con los que cuenta la organización ya que esta identificación es parte de la recolección de datos.

Existen 2 tipos de controles a identificar:

I. Controles requeridos: Implementados con base en reglas y procedimientos. En esta categoría se pueden incluir los señalamientos y anuncios que hay en las instalaciones, así como también a los registros que se llevan en los procesos de la organización, incluyendo bitácoras, listas de personal y usuarios, etcétera.

II. Controles discrecionales: Son establecidos comúnmente por los administradores con el propósito de reducir vulnerabilidades a un nivel aceptable. Este tipo de controles incluyen los reglamentos que los administradores pueden establecer en las distintas áreas de una organización.

4.3.6 DETERMINAR LOS RIESGOS RESIDUALES (CONCLUSIONES)

Esta parte consiste en obtener el riesgo residual que arroja el análisis y determinar si es aceptable o no para la organización. El riesgo residual consiste en una serie de conclusiones alcanzadas en el proceso de evaluación de la organización. Estas conclusiones deben identificar los siguientes aspectos:

- Áreas que tienen alta vulnerabilidad junto con la probabilidad de ocurrencia de una amenaza. Estas áreas son las que necesitan con más urgencia mecanismos de seguridad que ayuden a reducir sus vulnerabilidades y por lo tanto reduzca la probabilidad de ocurrencia de las amenazas identificadas en dichas áreas.

- Todos los controles que no están dentro del lugar. Este aspecto sirve para saber qué controles no se encuentran instalados en las áreas analizadas y si son necesarios para la organización, de esta manera, se procede a implementar los controles elegidos para su implementación.

El resultado de este paso permite seleccionar los controles adicionales de la organización.

4 3.7 IDENTIFICAR LOS CONTROLES ADICIONALES (RECOMENDACIONES)

En esta parte, se identifica la manera más efectiva de reducir los riesgos además de determinar cuál es la manera menos costosa para llevarlo a cabo.

Esto se realiza con base en los controles adicionales implementados, los cuales son:

- Recomendaciones de controles requeridos: Son aquellos que no se encuentran aún implementados en la organización pero que son requeridos.

- Recomendación de controles discrecionales: Son controles necesarios para reducir el nivel de riesgo.

4.3.8 PREPARAR UN INFORME DEL ANÁLISIS DE RIESGOS

Una vez que el análisis de riesgo está completo, es necesario preparar un informe detallado con los resultados que se evaluaron durante el análisis de riesgo. En este informe se indica si los controles de seguridad de la organización son efectivos.

Se aplica tanto a los activos críticos como a nivel organizacional hasta alcanzar el nivel de seguridad adecuado.

Los detalles técnicos del reporte debe incluir por lo menos los siguientes puntos:

- Un análisis de los riesgos que mide posibles pérdidas para la organización.

- Un análisis de amenazas cuya ocurrencia puede producir pérdidas.

- Ambiente usado en la realización del análisis.

- Conexión del sistema.

- Nivel o niveles de sensibilidad de los datos.
- Riesgo residual expresado en una base individual de vulnerabilidad.
- Un análisis de los riesgos que mide posibles pérdidas para la organización.
- Un análisis de las medidas de seguridad que actuarían como una protección.
- Cálculos detallados de la expectativa de la pérdida anual.

Promover la realización de análisis de riesgo continuos permite determinar requerimientos e incrementar el nivel de seguridad de una organización, todo esto se plasma en el informe final del análisis de riesgo.

CAPÍTULO 5

Análisis de Riesgo de los siete Departamentos

INTRODUCCIÓN

A continuación se desarrolla paso a paso el análisis de riesgo de cada uno de los siete departamentos. Para su realización, se efectuaron visitas a los departamentos correspondientes para poder recopilar evidencias necesarias que permitieron el desarrollo del proyecto. Además se diseñaron y aplicaron cuestionarios al personal de cada departamento para obtener información que base para un análisis completo y confiable.

Se supervisaron actividades de los departamentos para evaluar el funcionamiento de los mismos, además de cotejar información e ideas con los encargados y personal de los departamentos.

Con la información y las evidencias necesarias se procedió a realizar el análisis de riesgo siguiendo los ocho pasos explicados en el capítulo anterior, obteniendo como resultado lo que está a continuación.

5.1 DEPARTAMENTO DE COMPUTACIÓN[15]

Se encuentra conformado por diversos laboratorios y cubículos del personal que labora en esta área, a continuación se describen éstos, mencionando la administración de los equipos de red que involucran:

a) Laboratorio de redes y seguridad

Al ser éste un laboratorio enfocado a redes y seguridad, cuenta con su propio servidor además de contar con un switch para la red del laboratorio y fines académicos. El servidor y el switch son administrados por los encargados del laboratorio. En cada clase dependiendo del profesor, éste puede modificar algunas configuraciones del equipo de red con fines académicos.

b) Laboratorio Intel

El laboratorio cuenta con su propio servidor el cual es administrado por el encargado general del laboratorio.

c) Programa de Tecnología en Computación (PROTECO)

Esta sala cuenta con sus propios servidores y equipos de red administrados por los encargados de la sala. El equipo se encuentra fuera del alcance del alumnado y sólo tiene acceso a éste el personal autorizado.

[15] Véanse los cuestionarios en el apéndice D y en el apéndice E las estadísticas y el análisis de resultados

d) Laboratorio de computación Salas A y B

Estas dos salas tienen red que es proveída por servidores propios que son administrados por los encargados de las salas y a los cuales el alumnado no tiene acceso.

e) Laboratorio de Cómputo "Sala C"

Este laboratorio cuenta con dos tipos distintos de servidor, ambos administrados por el encargado de la sala: servidor RS 6000 y servidor de bases de datos, archivos

f) Laboratorio de Multimedia

Laboratorio con servidor propio operado y configurado por su encargado.

g) Cubículos del departamento

Los cubículos del departamento son ocupados por profesores del área y empleados del mismo. Estas áreas cuentan con servicios de red los cuales son administrados por el mismo encargado del laboratorio sala C. Se comentó en las entrevistas que en algunas ocasiones se había suscitado un caso de denegación de servicios y puertos por parte de la administración de servicios de red sin previo aviso.

5.1.1. IDENTIFICACIÓN DE ACTIVOS

El departamento está compuesto por laboratorios y cubículos en los cuales se encontraron los siguientes activos:

a) Laboratorio IBM: Equipos de cómputo

b) Laboratorio de dispositivos lógicos programables: Equipos de cómputo, Tarjetas Xilinx, Software (Altera Max Plus, Xilinx, etcétera)

c) Laboratorio de Dispositivos Entrada y Salida: Osciloscopio, generador servidores, fuente de poder, multímetro, computadoras.

d) Laboratorio de Redes y Seguridad: Servidor, switch.

e) Laboratorio Intel: Servidores, computadoras, mobiliario, artículos personales.

f) Laboratorio de Microcomputadoras: Computadoras, fuentes de voltaje, tarjetas de desarrollo, multímetro, osciloscopio.

g) Programa de Tecnología en Computación (PROTECO): Computadoras, servidores, firewall, energía eléctrica

h) Laboratorio de Investigación para el Desarrollo Académico (LINDA): Energía eléctrica, herramientas de trabajo (esmeril, taladro, etcétera), robots, computadoras, microondas, osciloscopio

i) Laboratorio de computación Salas A Y B: Equipos de cómputo, energía eléctrica, servidores

j) Laboratorio de computación Sala C: Computadoras, servidor RS 6000, servidor de Bases de datos, archivos

k) Laboratorio de Investigación y Desarrollo de Software Libre (LIDSOL): Computadoras.

l) Laboratorio de Multimedia: Servidores, la información contenida en los servidores, impresoras, computadoras

m) Cubículos: Comprobantes académicos (diplomas, constancias, etcétera.) computadora y accesorios, libros, artículos de papelería, información, impresora, objetos personales, apuntes, respaldos.

5.1.2. IDENTIFICACIÓN DE AMENAZAS

a) Laboratorio de IBM

Este laboratorio en general no maneja ninguna información relevante, se utiliza para dar cursos o dar servicio a profesores en caso de que requieran hacer uso de este laboratorio para alguna clase en específico.

Una de las amenazas más graves que podría~~n~~ presentarse es el robo de equipo del laboratorio, el cual representa el costo mayor de esta área y en él se mantiene información utilizada en las actividades del departamento. Además de esto se tiene el robo de información.

Uno de los problemas que se han presentado en este laboratorio según las entrevistas es que en alguna ocasión, algunos alumnos intentaron romper algunas claves de acceso, sin embargo, se localizó la falla y se actuó de una manera rápida y eficaz.

b) Laboratorio de dispositivos lógicos programables

La información que se maneja en este laboratorio en general es el uso de programas de diseño digital como son xilinx y altera max plus, se mencionó que

los activos más importantes en el laboratorio son las tarjetas xilinx y el equipo de cómputo, por lo que la amenaza más grave es el robo de este tipo de equipo.

Los problemas que se presentan con mayor frecuencia en este laboratorio es que los alumnos insertan memorias usb en los equipos de cómputo y muchas veces existe la amenaza de contaminar con virus al equipo de laboratorio.

Otro amenaza es que los alumnos llenan el disco duro de los equipos al realizar sus actividades con el equipo xilinx ocasionando la saturación del equipo de cómputo.

c) Laboratorio de dispositivos Entrada y Salida

En este laboratorio se manejan equipos electrónicos de medición como el osciloscopio, fuentes de poder y computadoras.

En este laboratorio si denegaran los puertos no se vería atentado ningún servicio, ya que las computadoras no necesitan salida a internet.

La mayor amenaza en este laboratorio, al igual que en los anteriores, es el robo de equipo, las fallas de energía y la infección de los equipos por medio de virus informáticos.

d) Laboratorio de redes y seguridad

Este laboratorio maneja información relacionada con las asignaturas de redes.

Las principales amenazas son: fallas con algunos equipos (respecto al rendimiento), fallas de energía, así como problemas con virus y la denegación de puertos en el equipo.

e) Laboratorio Intel

Este laboratorio maneja información relacionada con Windows, Linux, Bases de datos Oracle y herramientas de desarrollo para procesamiento paralelo.

Las amenazas comprenden la suspensión de servicios fundamentales para la realización de las actividades dentro del laboratorio, así como la denegación de puertos en el equipo, las fallas de energía eléctrica y el robo de información en los equipos.

f) Laboratorio de microcomputadoras

Este laboratorio maneja información de software y hardware relacionada con microcontroladores, por lo que las principales amenazas son fallas con algunos equipos sobre todo con las tarjetas de evaluación de microcontroladores. También se debe contemplar el robo de equipo y las fallas de energía eléctrica.

g) Programa de tecnología en computación (PROTECO)

En este laboratorio se maneja información académica y desarrollo de proyectos personales de becarios, aplicaciones para ingeniería y de docencia (impartición de cursos) con el fin de que los alumnos pertenecientes al programa de tecnología en cómputo desarrollen sus habilidades de programación.

Entre las principales amenazas que pueden presentarse se encuentran la denegación de servicios fundamentales para la realización de las actividades en el laboratorio, tales como la denegación de puertos, además del ya mencionado robo de equipo, fallas eléctricas, robo de información.

h) Laboratorio de investigación para el desarrollo académico (LINDA)

El tipo de información que se maneja es de distintos proyectos de software y hardware, robótica, botánica, proyectos multidisciplinarios.

Las amenazas en este laboratorio sólo contemplan el robo de equipo y las fallas de energía eléctrica.

i) Laboratorio de computación Salas A Y B

El tipo de información que se maneja es meramente académica y de docencia.

En cuanto a los problemas que se han presentado en esta área y que representan las amenazas se encuentra el robo de equipo. También se mencionó alguna sobrecarga y el fallo del suministro de energía una o dos veces al año.

j) Laboratorio de investigación y desarrollo de software libre (LIDSOL)

El tipo de información que se maneja es de proyectos personales y tareas, por lo que las amenazas que se pueden presentar sólo contemplan el robo de equipo y las fallas de energía eléctrica.

k) Laboratorio de computación sala C

En este laboratorio se da el servicio de préstamo de computadoras, impresión de trabajos académicos, servidor de archivos, además de que se cuenta con bases de datos.

Se presentan amenazas de robo de equipo, infección de virus, fallas de energía eléctrica y robo de información.

l) Laboratorio de multimedia

En este laboratorio se maneja información de alumnos; calificaciones y asistencia, además que provee el servicio de correo electrónico a ciertos profesores. Si se denegaran los puertos se contra la disponibilidad del servicio, ya que el servicio de correo electrónico necesita de un puerto para dar servicio. Además está presente también la amenaza de robo de equipo.

m) Cubículos

En general las amenazas que presentaron los cubículos de profesores contemplan el robo de material dentro de los cubículos, las fallas de energía eléctrica, denegación de puertos y servicios y problemas con correos electrónicos no deseados.

5.1.3. IDENTIFICACIÓN DE VULNERABILIDADES

a) Laboratorio de IBM

En el laboratorio no cuentan con algún registro para el control de acceso, cada profesor se hace responsable del uso de este laboratorio.

Debido a que éste es un laboratorio que maneja software libre no tienen actualizados sus parches de seguridad.

Otra vulnerabilidad evidente es respecto al control de acceso, ya que las chapas de las puertas son muy sencillas, con lo que se podrían manipular fácilmente.

Falta personal que labore en ese laboratorio, este personal debe ser contratado directamente por la institución, y por más que se ha solicitado, no se ha dado respuestas a esto.

b) Laboratorio de dispositivos lógicos programables

Refiriéndose al control de acceso, manejan una bitácora para poder registrar tanto a alumnos como al personal del laboratorio.

No todo el equipo de cómputo cuenta con antivirus ni acceso a la red, los equipos que cuentan con acceso a la red, actualizan los antivirus automáticamente y cuando existe algún problema con algún equipo de cómputo lo que se hace es cambiar uno por otro para reparar el daño.

Hablando del mantenimiento del laboratorio, se hace limpieza cada semana de forma general a los equipos y hablando de software cada semestre se hace una actualización y depuración del equipo. En caso de que llegaran a tener una falla,

refiriéndose al soporte técnico, los encargados de resolver estos problemas son la gente del departamento.

c) Laboratorio de dispositivos Entrada y Salida

El control de acceso en este laboratorio depende del profesor en su hora de clase y cuando el laboratorio se encuentra abierto a todos los alumnos, el encargado lleva un registro.

Las computadoras cuentan con antivirus pero no tiene ni las actualizaciones ni los parches necesarios.

d) Laboratorio de redes y seguridad

Los principales problemas que se han presentado son fallas con algunos equipos (respecto al rendimiento), así como problemas con virus y gusanos; así como también la denegación de puertos en el equipo lo cual representa una gran vulnerabilidad tomando en cuenta que el laboratorio basa la mayor parte de sus actividades en el uso de los puertos de los equipos. Las posibles fallas eléctricas que se puedan generar y que puedan dañar la información debido a que no todos los equipos cuentan con no-breaks.

e) Laboratorio Intel

Las principales vulnerabilidades que se presentan son la suspensión de servicios fundamentales para la realización de las actividades dentro del laboratorio, como la denegación de puertos en el equipo de cómputo, así como la ventilación con la que se cuenta es muy débil para los equipos que se manejan.

f) Laboratorio de microcomputadoras

La principal vulnerabilidad en este laboratorio es que su control de acceso es casi nulo ya que al no ser utilizado para clases, el laboratorio está abierto y no hay personal que supervise las actividades que se realizan en ese momento.

g) Programa de tecnología en computación (PROTECO)

No se cuenta con un control de acceso adecuado ni con soporte técnico en caso de presentarse alguna falla en el equipo; es posible ocasionar un incendio ya que el personal que ahí labora en ocasiones juega con cosas que pueden ser peligrosas para la seguridad tanto del laboratorio como de las personas en sí y el extinguidor existente posiblemente haya caducado. Nunca se ha usado, pero tampoco se revisa si está en condiciones óptimas.

h) Laboratorio de investigación para el desarrollo académico (LINDA)

Las vulnerabilidades en este laboratorio se reducen a las posibles fallas eléctricas que se puedan generar y que puedan dañar la información debido a que no todos los equipos cuentan con no-breaks.

i) Laboratorio de computación Salas A Y B

El control de acceso en este laboratorio no es tan robusto como debiera ser y se han presentado robos debido a esta vulnerabilidad.

j) Laboratorio de investigación y desarrollo de software libre (LIDSOL)

Se encontraron vulnerabilidades como el deterioro de la puerta de entrada que ya no cierra correctamente, los contactos no están aterrizados y esto causa bajas de energía y no hay condiciones de temperatura adecuadas para el equipo de cómputo que se maneja en esta área.

k) Laboratorio de computación sala C

Se cuenta con un sistema de registro para los alumnos; este registro se puede observar directamente en la base de datos. Los usuarios de esta sala se autentican por medio de una credencial en la entrada, y se les asigna una clave de red cada semestre. Los respaldos se realizan en DVD´s o discos duros periódicamente, por lo que no se encontraron vulnerabilidades en el aspecto de robo de equipos o pérdida de información.

l) Laboratorio de multimedia

Se cuenta con un sistema de autenticación para los alumnos (login y password). Estas cuentas cuando ya no se encuentran en uso son borradas, se proporcionan solamente cuando se realizan cursos ya sea en clases o intersemestrales, también los prestadores de servicio social y empleados son administrados mediante calves de red. A pesar de este control de acceso, el laboratorio ha sufrido robos.

El equipo de cómputo no posee antivirus, se tiene un proxy en el servidor. Los respaldos se realizan en CD’s periódicamente.

m) Cubículos de profesores

Vulnerabilidades en los cubículos tienen que ver con fallas eléctricas que no son controladas al no contar con un no-break.

También se reportan robos de equipo de cómputo, falta de material de papelería (hojas, engrapadora).

El área de cubículos se encuentra dividida en 2 partes, en las cuales el control de acceso no es parejo; por un lado una de las partes cuenta con una puerta con 5 chapas, la cual, sin embargo, está abierta la mayor parte del tiempo sin control alguno. La otra parte de los cubículos se encuentra resguardada con una puerta que sólo se abre por dentro y que cuenta con timbres en su parte exterior.

5.1.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

Hasta ahora el impacto de las amenazas en cada área del departamento no ha ocasionado pérdidas muy grandes. El problema con los controles de acceso ha ocasionado pérdida de equipo pero con un costo muy bajo, sin embargo, los laboratorios se actualizan con nuevo equipo y es necesario incrementar el control de acceso.

El nivel de daño en los equipos por fallas eléctricas aún no ha ocasionado pérdida material ni de información. De igual manera, los casi nulos ataques informáticos que se han presentado se han detectado y no han causado pérdidas en la información que es el activo del departamento.

Un punto que sí ha causado problemas es la denegación de servicios que se ha presentado en cubículos de profesores del departamento, la cual detiene actividades del área.

5.1.5. CONTROLES EXISTENTES

a) Laboratorio de Microcomputadoras: Cámaras de vigilancia

b) Laboratorio de Redes y seguridad: Control de acceso (registro), puertas con doble cerradura, no- break

c) Laboratorio de Intel: Control de acceso, software apropiado

d) Laboratorio de Multimedia: Control de acceso (registro), nombre de usuario con contraseña

e) Laboratorio de Dispositivos Lógicos Programables: Acceso con credencial, bitácora, doble cerradura en la puerta

f) Laboratorio de Dispositivos de Entrada y Salida: Doble cerradura en la puerta

g) Laboratorio IBM: Doble cerradura en la puerta, una cerradura de alta seguridad, control de acceso biométrico

h) Laboratorio de computación sala C: Extinguidores, control de acceso (registro)

i) Laboratorio PROTECO: No cuentan con control de acceso, firewall y antivirus

j) Laboratorio LINDA: Control de acceso (registro), Extinguidores

k) Laboratorio de computación salas A Y B: Control de Acceso (registro), firewall y Antivirus

l) Laboratorio LIDSOL: Control de acceso (registro), firewall, extinguidores

m) Cubículos: algunos cuentan con: control de acceso, antivirus, no-break, varias cerraduras en la puerta del cubículo, nombre de usuario y contraseña en los equipos de cómputo.

5.1.6. RIESGOS RESIDUALES

El riesgo residual principal que presenta el departamento es el del robo de equipo que puede presentarse debido a que en algunas de las áreas de trabajo no se tiene un control de acceso suficiente para evitar que ocurra.

También está el riesgo del daño de información y equipos debido a fallas de energía eléctrica, ya que no todo el departamento cuenta con no-breaks.

5.1.7. CONTROLES ADICIONALES

Aunque algunos laboratorios cuentan con su reglamento, es indispensable que todos elaboren uno y se encuentre a la vista de los usuarios que ingresan en el lugar, de esta manera las personas estarán conscientes de las reglas que deben seguirse en todo momento.

a) Laboratorio IBM

- Manejar en la puerta de la entrada chapas de seguridad más eficientes, para que no sean tan fáciles de manipular.
- Convendría no darle a tanta personas la autorización para entrar al laboratorio o actualizar periódicamente estos permisos.
- Contratar más personal para que este laboratorio pueda dar un mejor servicio.
- Con el personal suficiente; tener a varios encargados en turnos diferentes para que puedan implementar un control de acceso y se pueda dar servicio en este laboratorio con un nivel de seguridad apropiado

b) Laboratorio de Dispositivos Lógicos Programables

- Se debe advertir a todo el alumnado que no se puede grabar nada de información en los equipos de cómputo, simplemente se deben usar las memorias usb para poder realizar sus trabajos.

- Hablando del control de acceso, las chapas de la puerta son muy viejas, lo que podría ser un gran peligro, ya que éstas son muy fáciles de manipular y por consiguiente, cualquier intruso podría acceder a este laboratorio. Se recomienda poner chapas nuevas de alta seguridad y si fuera posible, cámaras de vigilancia para poder monitorear las entradas y salidas de toda la gente en este lugar.

- Por último el personal del laboratorio debe divulgar más sus políticas de seguridad, ya que solamente poner un letrero en las paredes hecho a mano y nada notorio no es suficiente.

c) Laboratorio de Dispositivos de Entrada y Salida

- Se deben dar a conocer las políticas de seguridad a los usuarios, con carteles visibles en el laboratorio, así como asegurarse que los profesores las divulguen a sus alumnos.

- El control de acceso se incrementaría asegurando la entrada al laboratorio, ya que sólo se cuenta con una chapa

- Todo el equipo obsoleto se debe retirar del laboratorio ya que reduce el espacio de trabajo de los usuarios.

- Se sugiere contar con un supresor de voltajes para evitar sobrecargas en los equipos.

- La realización del mantenimiento preventivo periódicamente en los equipos por parte del personal especializado se debe realizar para evitar mayores costos por pérdida total de equipos.

- Los equipos de cómputo deben ser actualizados ya que con los que se cuenta son obsoletos y no tienen funcionalidad.

- Evitar tener mobiliario ajeno al laboratorio, ya que se observó que se tienen monitores descompuestos, tener en cuenta que se trata de un laboratorio y no de una bodega.

- Tener un extinguidor debido a que existe la amenaza de un corto circuito porque se trabaja con equipos electrónicos.

d) Laboratorio de Redes y Seguridad

- En lo que se refiere a hardware y software se observó que los dispositivos se encuentran en buen estado, lo cual habla de un buen mantenimiento, se sugiere que la información que manejan cuente con un respaldo para prevenir posibles pérdidas, las cuales pueden ser provocadas por incendios, fallas eléctricas o por virus.

- Con lo que respecta a los mecanismos de seguridad y políticas se observó que son adecuadas, ya que se cuenta con la difusión de las políticas dentro del laboratorio al igual que en su página web. Se sugiere mantener al personal informado ante las medidas y cambios que se hagan respecto a la seguridad tanto en el departamento, como en el laboratorio.

e) Laboratorio de Intel

- En lo que se refiere al control de acceso, se encontraron ciertos inconvenientes ya que no se cuenta con una bitácora que registre la entrada y salida de los alumnos.

- Por otra parte, en lo que se refiere a hardware y software, se observó que los dispositivos se encuentran en buen estado lo cual habla de un buen mantenimiento, se sugiere que la información que manejan cuente con un respaldo para prevenir posibles pérdidas las cuales pueden ser provocadas por incendios, fallas eléctricas o por virus.

- Con lo que respecta a los mecanismos y políticas de seguridad se observó que son adecuadas, ya que se cuenta con la difusión de las políticas dentro del laboratorio al igual que en su página web. Se sugiere mantener al personal informado ante las medidas y cambios que se hagan respecto a la seguridad tanto en el departamento, como en el laboratorio.

f) Laboratorio de Microcomputadoras

- Se sugiere implementar una bitácora en la cual se registren las entradas y salidas tanto de profesores como de alumnos.

- Por otra parte, en lo que se refiere a hardware y software, se observó que la mayoría de equipos son obsoletos dado que cuentan con un hardware insuficiente, pues no contienen entradas de usb, unidad de cd, etcétera. Se sugiere al personal encargado que todo el equipo en desuso sea removido del laboratorio para una buena adecuación.

- Es recomendable que se publiquen o difundan las políticas de seguridad en el laboratorio

g) Laboratorio PROTECO

- Es importante que cualquier cambio que se desee realizar con respecto a la administración de los servicios sea previamente anunciado, para que de esta manera el personal que labora en el laboratorio tome sus medidas de precaución y no se vea afectado en la realización de su trabajo por la denegación de los servicios que provee el laboratorio.

- Es indispensable contar con un control de acceso adecuado ya que se puede observar que todos pueden entrar siempre y cuando haya un miembro perteneciente al laboratorio, aunque no se ha presentado ningún connato que ocasione la pérdida de los bienes que son importantes para el laboratorio salvo el robo de un mouse, no está de más tomar una medida de control que permita al responsable del laboratorio saber quién entra y sale.

- Se recomienda verificar que el extinguidor que existe dentro del laboratorio se encuentre en óptimas condiciones.

- Como se cuenta con un firewall como medida de prevención contra ataques, se recomienda verificar que esté bien configurado para evitar otros posibles ataques.

h) Laboratorio LINDA

- Una de las vulnerabilidades del laboratorio es el exceso de confianza, aunque no han sufrido robos, es necesario contar con algún control de acceso suficiente como para saber quiénes son miembros y quiénes visitan el laboratorio.

- Revisar que el extinguidor se encuentre en condiciones óptimas para ser usado en caso de un incendio.

i) Laboratorio de computación salas A Y B

- Se sabe que los servidores cuentan con un no-break en caso de que se suspenda el suministro de energía eléctrica, pero los equipos de cómputo no cuentan con uno, esto ha ocasionado que algunos equipos se desconfiguren. Se sugiere que cada equipo cuente con un no-break para evitar pérdidas de información y daños a los equipos de cómputo.

- Manejar en las puertas de entrada de los cubículos 1, 2 y 3 chapas de seguridad más eficientes, para que sólo los encargados tengan acceso a éstos

j) Laboratorio LIDSOL

- Se sugiere cambiar las 3 chapas de la puerta del laboratorio ya que esto ha ocasionado que se roben algunas cosas como objetos personales. Así como corregir la conexión de los contactos, es decir; aterrizarlos pues al no estarlo, ocasionan daños a los equipos de cómputo así como bajas de energía que pueden provocar que una fuente se queme.

k) Laboratorio de computación sala C

- Se deben dar a conocer las políticas de seguridad a los usuarios con carteles visibles en el laboratorio, además de asegurarse que todos los miembros del laboratorio las conozcan y las divulguen.
- Se debe de dar mantenimiento al equipo de cómputo al igual que a las aplicaciones de software periódicamente.
- Es importante tener un control de acceso del personal, ya que en un ataque interno esta información puede ser primordial.
- Evitar que personas ajenas al laboratorio tengan acceso, como familiares, hijos, amigos de los empleados.
- Es conveniente tener una buena limpieza de escritorio dentro del laboratorio.

l) Laboratorio Multimedia

- Se deben dar a conocer las políticas de seguridad a los usuarios con carteles visibles en el laboratorio, además de asegurarse que todos los miembros del laboratorio las conozcan y las divulguen, ya que se observó que hay total desconocimiento.
- Mejorar el control de acceso, asegurando la entrada al laboratorio, tener una bitácora de registro de entrada y salida.
- Instalar antivirus y firewall en todas las computadoras al igual que instalar las actualizaciones adecuadas periódicamente.
- Tener respaldo de la información del servidor, así como realizar análisis forense de los ataques para determinar los puntos vulnerables en el servidor y evitar los ataques.
- Realizar el cableado estructurado según las normas EIA/TIA 568 y 569, ya que se observó una mala implementación.

- Evitar que personas ajenas al laboratorio tengan acceso, como familiares, hijos, amigos de los empleados.
- Reparar la cámara de seguridad de la entrada así como monitorearla, ya que ésta sería muy útil para el control de acceso.
- Llevar un inventario de los bienes, para poder darse cuenta de cualquier robo.
- Evitar tener mobiliario ajeno al laboratorio, ya que se observó que se tienen muebles como mesas, sillas que obstruyen la entrada.
- Tener un plan de contingencia en caso de un ataque, ya que cuando fueron victimas de un ataque no tuvieron un plan.

m) Cubículos

- El uso de antivirus y antispyware es esencial para el funcionamiento adecuado del equipo de cómputo en el cubículo, por lo que es necesario que se brinde a los cubículos el software necesario para proteger la información que se maneja en ellos.
- El acceso a los cubículos que se encuentran en una parte del edificio tiene un resguardo de 5 chapas, además de una chapa digital; el problema es que la puerta se encuentra abierta por mucho tiempo haciendo que las chapas manuales y digitales pierdan completamente el poder de resguardar el acceso, por lo tanto se debe mantener cerrada la puerta tal y como sucede en la parte opuesta del edificio, en donde la puerta que da acceso a los cubículos se encuentra cerrada.
- La puerta de acceso a la otra área de cubículos permanece cerrada, sin embargo, cuando alguien toca el timbre de acceso se puede acceder sin necesidad de identificarse. Es necesario que el personal visitante desconocido se identifique y/o registre a la entrada del área de los cubículos.
- El buen cuidado del equipo de cómputo es indispensable para que el trabajo dentro del cubículo se pueda llevar a cabo; por lo que el contar con un no-break es de vital importancia no sólo para el cuidado del equipo, sino para el resguardo de la información que se maneja.
- Se debe proveer a los cubículos con el material indispensable para llevar a cabo correctamente su trabajo. El material de papelería tiene que estar siempre al alcance de todo el personal que labora en los cubículos.

- El correo spam es un problema que debe ser atendido principalmente por el administrador de la red. Se deben utilizar herramientas y protocolos que eviten esta potencial amenaza de virus en los cubículos.

- La denegación de puertos implica la interrupción de alguna actividad en el cubículo que pudiera ser de vital importancia, por lo que esta acción debe ser acompañada siempre por un previo aviso con el suficiente tiempo para que el personal que labora en el cubículo esté preparado. Dicho aviso debe explicar las razones de la denegación y el tiempo que durarán los puertos en ese estado.

5.2 DEPARTAMENTO DE CONTROL[16]

El departamento de control es responsable de los siguientes laboratorios:

a) Laboratorio de control analógico y digital

b) Laboratorio de circuitos eléctricos

c) Laboratorio de robótica

d) Laboratorio de modos de deslizamiento

e) Laboratorio de ingeniería biomédicas

f) Sala de computación

g) Además tiene bajo su control los cubículos del departamento que son alrededor de 20

5.2.1. IDENTIFICACIÓN DE ACTIVOS

Los activos que se manejan en este departamento son los siguientes:

- Información que se maneja a nivel personal, que se encuentra almacenado en la computadora de cada profesor, no se cuenta con un respaldo general.

- Información que se encuentra en el servidor, principalmente la página del departamento donde se publican artículos, actividades y archivos relacionados con la docencia como prácticas y manuales.

[16] Véanse los cuestionarios en el apéndice D y en el apéndice E las estadísticas y el análisis de resultados

- Activos como computadoras, escáners, impresoras y servidores.
- Cosas personales como bocinas, laptops, libros, mochilas, bolsas de mano y portafolios.

En caso de que exista la pérdida de alguno de los activos, puede observarse lo siguiente:

- Como la información es personal, cada dueño del equipo le da un nivel de importancia. Si cuenta con un respaldo, la pérdida se reduce al equipo, el cual ya no es recuperado tan fácilmente pues depende del presupuesto del departamento.
- En el caso del servidor, la información es respaldada, si ésta borra o altera se procede a restaurar el servidor formateando e instalando los componentes originales. La pérdida se reduce al equipo, el cual difícilmente puede recuperarse.
- Cosas personales, como no se lleva un control de las mismas, la pérdida es definitiva y nadie es responsable de éstas.

Los activos, así como su nivel de importancia, cantidad y acciones que se realizan en caso de pérdida, pueden observarse en las tablas 5.1 y 5.2

Tabla 5.1 Activos

Activo	Nivel de Importancia	Contenido	Tipo de acceso	Acciones en caso de pérdida
Computadora Personal	Personal	Información personal como: Documentos personales, proyectos, música, notas, listas, videos educativos.	Personal	Se levanta un acta para notificar a las autoridades. La información se recupera dependiendo de cada persona, no se tiene un respaldo general. Para el equipo probablemente se recupera en el siguiente presupuesto.
Servidor	Alto	Contiene la	Privado	En caso de

		página del departamento y archivos relacionados con la docencia.	(Administrador)	pérdida, la página no podría estar disponible, se levanta un acta, en caso de ataque el servidor es restaurado.
Computadoras de Laboratorio	Medio	Software de trabajo, y documentos de alumnos	Público por medio de clave, en algunos caso no.	Se levanta un acta para notificar a las autoridades, en cuanto a la información ésta se pierde en su totalidad.

Tabla 5.2 Activos

Activo	Cantidad	Antivirus y firewall	Cuentas de Acceso
Computadora personal	20	19	Todas
Computadora de Laboratorio	140	160	Algunas
Otros (impresoras, scanner, reguladores)	20	No Aplica	No Aplica
Objetos personales	No Aplica	No Aplica	No Aplica

5.2.2. IDENTIFICACIÓN DE AMENAZAS

Las amenazas que se encontraron en este departamento se pueden clasificar de la siguiente manera:

- **Humanas:** El robo de información personal debido al control de acceso que se tiene.
- **Errores de Hardware:** Los equipos por tanto tiempo de uso dejan de funcionar adecuadamente total o parcialmente.
- **Errores de red:** Posible infección de los equipos por virus, saturación de puertos.

- **Problemas de tipo lógico:** Software malicioso, software mal intencionado.

- **Naturales:** Terremotos, fallas eléctricas.

Las amenazas más frecuentes son las de tipo lógico y las humanas, por periodos las naturales.

5.2.3. IDENTIFICACIÓN DE VULNERABILIDADES

Las vulnerabilidades que se encontraron en este departamento se pueden clasificar de la siguiente manera:

- **Física:** Dejar la puerta abierta, no contar con cámaras suficientes, no contar con registro de acceso.

- **Hardware:** No leer los manuales, no considerar las características del dispositivo.

- **De red:** Dejar puertos de comunicaciones abiertos, mala configuración del firewall.

- **Naturales:** No se cuenta con suficientes extinguidores.

La vulnerabilidad más frecuente es la de tipo física.

5.2.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

El robo de un equipo conlleva a la pérdida de la información personal, si el dueño tiene un respaldo de la información, las pérdidas se reducen a sólo el equipo, el cual es reportado por medio de un acta dirigida a las autoridades, el equipo rara vez es recuperado.

En el caso de robo de información si ésta es confidencial se puede hacer mal uso de ella, reutilizándola de mala manera, inclusive presentándola en su nombre, forzando así a la publicación más temprana del proyecto.

En caso de amenazas naturales, el equipo puede y no recuperarse.

Para las amenazas de tipo lógico, si el antivirus no previene, corrige o detecta el ataque, el equipo puede sufrir daños.

Se presenta pérdida temporal de los servicios que ofrece el servidor cuando ocurren ataques, debido a que es necesario hacer respaldos y formatear el equipo.

5.2.5. CONTROLES EXISTENTES

Los controles que se encontraron son de carácter general:

Requeridos:

- Todas las computadoras cuentan con un antivirus activado y constantemente actualizado. Nota: existe una computadora que por limitaciones de software y hardware no se le puede instalar un antivirus.
- Todas las computadoras tienen activado el firewall de Windows
- En el caso de los cubículos, éstos cuentan con dos chapas, las llaves de dichas chapas están bajo control del responsable de cada cubículo.
- Para cada laboratorio existe un responsable por turno.
- Se cuentan con cámaras en los edificios, una en cada piso y una en el estacionamiento.

Discrecionales:

- No dejar las puertas abiertas
- En caso de salir, dejar cerrada la sesión de usuario
- No fumar dentro de un área determinada para evitar incendios.
- Poner una chapa extra a la puerta.

5.2.6. RIESGOS RESIDUALES

En este caso se identifica que aunque existan medidas de seguridad implementadas dentro del departamento de control, no se debe pasar por alto que continuamente los riesgos están latentes aun cuando no se les pueda identificar, esto conduce a tener que fortalecer los controles o implementar nuevos para que los riesgos que se encuentran latentes sean mucho menores.

Entre los riesgos residuales identificados están:

- El control de acceso al departamento en general es aceptable pero aún con las medidas de seguridad existentes no es posible contrarrestar este riesgo, para esto se debe tener en cuenta que es posible implementar nuevos controles ya sea de manera obligatoria o de manera no obligatoria,

ya que esta implementación podría resultar muy costosa pero resultaría más efectiva porque disminuiría las vulnerabilidades.

- Un riesgo residual sería el ataque a equipos debido a la vulnerabilidad de no tener un antivirus actualizado o un firewall activado.
- Se tiene como otro riesgo residual las fallas eléctricas debido a la mala distribución de las estructuras eléctricas.
- El no controlar un incendio pequeño debido a no tener el buen funcionamiento de los extinguidores.

Ya identificados los riesgos residuales se deben tener controles adicionales para evitar riesgos o por lo menos reducirlos lo más posible haciéndolo a un nivel aceptable y disminuyendo las vulnerabilidades.

5.2.7. CONTROLES ADICIONALES

El principal problema que se presenta en el departamento, no radica en la seguridad sino en la falta de presupuesto, se pueden proponer muchas ideas, pero la implementación de la seguridad y el presupuesto van de la mano. Básicamente existen dos divisiones de controles adicionales las cuales son:

Los controles obligatorios, los cuales reducen los riesgos, son los siguientes:

- Se requiere la instalación de reguladores de voltaje y no-breaks para evitar las amenazas eléctricas, pero muchas veces el departamento opta por comprar con ese presupuesto otra máquina que es más necesaria.
- Recarga y buen funcionamiento de extinguidores.
- Configurar el firewall para restringir el acceso a sitios no seguros o prohibidos.
- Realizar actualización de antivirus de las computadoras.

Y los controles no obligatorios:

- Se pueden instalar timbres inalámbricos para solucionar el problema del control de acceso y el de las puertas abiertas.
- Chapas electrónicas, para solucionar el control de acceso, pero son demasiado caros y no existen los recursos necesarios.
- Cámaras infrarrojas y sensores de movimiento.

5.3 DEPARTAMENTO DE ELÉCTRICA DE POTENCIA[17]

Los servicios que se utilizan en el laboratorio, obtenidos en el cuestionario especial para el administrador son los siguientes:

- Intercambio de archivos entre los equipos
- Correo electrónico
- Consultas WEB

En lo que respecta a los equipos de los profesores de tiempo completo, se mencionó que sólo los utilizan para realizar consultas en línea y revisar sus correos electrónicos, por lo que se puede realizar un filtrado sobre los puertos sin mayor problema, garantizándoles una red más segura.

5.3.1. IDENTIFICACIÓN DE ACTIVOS

En estos dos laboratorios se identificaron, gracias a los cuestionarios y entrevistas que se realizaron, los siguientes activos:

- Libros de la materia
- Documentación importante (bitácoras de acceso, papeleo administrativo, etcétera.)
- Equipos de cómputo
- Periféricos
- Equipos activos
- Herramientas

En lo que respecta a las oficinas correspondientes a este departamento los activos importantes son:

- Libros de la materia
- Documentación importante (papeles administrativos, actas, etcétera.)
- Equipos de cómputo

[17] Véanse los cuestionarios en el apéndice D y en el apéndice E las estadísticas y el análisis de resultados

- ❖ Información digital (Documentos de planeación, exámenes, etcétera.)
- ❖ La salud de las personas (en especial en el área de máquinas de potencia).

5.3.2. IDENTIFICACIÓN DE AMENAZAS

Lo que se mencionó más frecuentemente, tanto en los laboratorios como en las oficinas, fue el temor al robo de equipos de cómputo. En estos casos no sólo se pierde toda la información importante que almacenan en éstos, sino que existe la gran pérdida monetaria que representan las computadoras y en el caso de los laboratorios, la denegación del servicio, pues es algo elemental para que puedan desarrollar sus prácticas los usuarios del lugar. En el caso de las oficinas, se pierden documentos administrativos, calificaciones, exámenes y esto representa una deficiencia en el trabajo de las personas que laboran en esta área.

Algunas amenazas que se identificaron en el laboratorio de máquinas eléctricas fueron: el daño a la integridad de las personas, actos de sabotaje en los equipos físicos para impedir la realización de ciertas prácticas y el robo de algunas herramientas propias del laboratorio, esto puede dañar el desempeño de las personas y propiciar la denegación del servicio tanto del laboratorio como administrativo.

Una amenaza muy importante que fue mencionada inmediatamente al hablar de un análisis de riesgo, fue la subestación que se localiza justo al lado de la oficina administrativa del laboratorio de maquinas eléctricas. Ésta representa una amenaza contra la salud de las personas que ahí elaboran por el ruido que ésta produce, el daño es gradual e irreversible. Además del daño por el constante ruido, existe el riesgo de una contingencia debido a la subestación y de acuerdo con el análisis, se encontró que no hay forma de salir en caso de incendio o de cualquier tipo de incidente. Esto representa una gran amenaza, pues en los días que se visitó el laboratorio, además de la mala planeación de las rutas de evacuación, se encontró una máquina obstruyendo el pasillo, esto significa aumentar el riesgo contra la integridad de las personas (Véase figura 5.1).

Figura 5.1 Mapa del Departamento de Electrónica de Potencia

Las fallas en el suministro eléctrico no ocurren de manera frecuente en esta división, por lo regular ocurren una vez o dos al año. En estos casos se pierde información y se pueden presentar daños en los equipos, sin embargo, las personas que se entrevistaron no le daban gran importancia a estos sucesos y decían que podían vivir con este riesgo sin que afectara en el desarrollo de su trabajo.

Cabe mencionar que uno de los ingenieros explicó que actualmente los fallos en el suministro eléctrico eran menores porque la institución es alimentada por dos anillos independientes y en caso que falle uno, el otro entrará en acción sin que se presenten fallas. Los cortes que más ocurren son los planeados, aunque también se mencionó que no había difusión en ese caso.

Los ataques de virus informáticos están latentes en todo equipo conectado a Internet y estadísticamente se puede ver que el personal tiene cierto desconocimiento acerca de las posibles fuentes de infección o sobre cómo actuar en caso de una.

5.3.3. IDENTIFICACIÓN DE VULNERABILIDADES

En el caso del robo de equipos, se identificaron algunas malas prácticas, por ejemplo, en las entrevistas se mencionó que mucha gente sale de sus oficinas dejando las puertas abiertas por periodos considerables de tiempo, dentro de los cuales, puede haber robo de equipos portátiles o dispositivos de almacenamiento.

Cuando se habla de sabotaje o de amenazas contra una persona o un laboratorio se está en un caso donde es muy difícil poder identificar la vulnerabilidad; en este análisis, ésta se encuentra en la falta de difusión de códigos de comportamiento o códigos de ética para todas las personas que laboran en estas instalaciones.

Una amenaza muy importante, es el daño que produce la subestación eléctrica, y claramente se puede determinar la vulnerabilidad en el mal diseño de la colocación de la oficina, al igual que el desconocimiento por parte de los diseñadores acerca de las repercusiones contra la salud que producen estos dispositivos.

Nótese que es evidente la falta de diseño en estas oficinas, como se muestra en la figura 5.1, pues no existen puertas de evacuación de emergencia hacia los exteriores, lo que representa que en caso de una contingencia puede haber muchos accidentes que podrían costar vidas humanas y todo esto por una mala planeación, lo que se define como vulnerabilidad.

En el caso del suministro eléctrico cabe mencionar que la falla se encuentra en la falta de difusión de los cortes programados por mantenimiento, sin embargo, también se debe considerar que en ese caso, la falta de UPS o no-break en los

equipos propicia situaciones como ésta, en donde puede haber pérdida de la información o daño en los equipos de hardware.

Considerando la vulnerabilidad de los virus informáticos, ésta radica en la falta de conocimientos acerca del tema, sin embargo, se puede mencionar que muchos de los usuarios de los equipos de cómputo tienen antivirus que se actualizan automáticamente vía internet.

5.3.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

Cuando se han cumplido ciertas amenazas, se tienen impactos que se deben catalogar en un análisis de riesgo para darles seguimiento y llevarlos a un punto aceptable.

En el caso de robo, no ha existido ningún caso propio en el departamento, por lo tanto el impacto no se puede medir, pero sí ha servido de ejemplo para implementar servicios de seguridad que garantice disminuir la vulnerabilidad o bien el departamento se ha hecho de buenas prácticas para que no sucedan estas acciones.

En el caso de sabotaje y amenazas contra personas y laboratorios, el impacto ha sido psicológico, pues algunas de las personas involucradas sienten poca seguridad en su lugar de trabajo, lo cual se nota en la entrevista.

También este tipo de situaciones ha creado denegación del servicio, en laboratorios, por ejemplo, debido al sabotaje en las maquinarias o bien al robo de la herramienta.

Lo que se refiere a la salud, es posible ver cómo la subestación ha dañado el sistema auditivo de uno de los encargados de las oficinas contiguas, debido al constante zumbido que se crea.

En el caso de la falla eléctrica, como su concurrencia es casi nula, considerado así por las personas que se entrevistaron, no existen grandes impactos, sólo pérdidas de archivos en el momento y cosas pequeñas que todos consideraron sin importancia.

En lo que se refiere a virus Informáticos, se tiene un solo caso de pérdida total de información valiosa, en ese caso el impacto fue alto y después de eso se implementaron controles para evitar que volviera a pasar.

5.3.5. CONTROLES EXISTENTES

Realmente no existen propiamente controles requeridos en los lugares que se visitaron, a excepción del Laboratorio de Eléctrica de Potencia donde existen bitácoras de visitas, en el resto de las oficinas y el otro laboratorio no existen.
En lo que se refiere a controles discrecionales, todas las oficinas y laboratorios lo tienen, buscando controlar el robo. En todas las oficinas se tienen al menos dos chapas, con llaves que sólo poseen los dueños del cubículo y nadie más.

Toda la información valiosa impresa (papeles administrativos, actas, exámenes, libros, etcétera) se encuentran resguardados en las oficinas de los dueños bajo algún tipo de mobiliario (mesas, archiveros o libreros) con algún tipo de chapa de las cuales sólo los dueños tienen las llaves y no las comparten con nadie, así como las llaves de sus oficinas.

En el caso de los virus informáticos, todos los usuarios tienen antivirus y algunos hasta algún tipo de firewall, buscando protegerse de este tipo de ataque, sin embargo, este control entra dentro de los discrecionales.

Se puede mencionar que el esquema de seguridad es casi nulo, pues no tienen definición de normas y políticas para el control de acceso, disponibilidad de sus áreas de trabajo y de los elementos que requieren.

5.3.6. RIESGOS RESIDUALES

Se debe mencionar que en la división a pesar de tener vulnerabilidades, están dispuestos a afrontar el riesgo que aún queda latente a pesar de implementar controles en el lugar donde laboran.

En el caso de las amenazas, dejaron de convertirse en ataques hace algún tiempo y a pesar de aún tener miedo a veces, aceptan el riesgo que queda y viven con él en todo momento.

Un riesgo residual muy alto es la falta de puertas de evacuación del laboratorio de Maquinas Eléctricas, sin embargo, no se ha implementado algún tipo de servicio que disminuya esa vulnerabilidad.

Cabe señalar que uno de los principales riesgos residuales que sigue siendo muy alto es el daño a la salud que produce la subestación, aún cuando el personal se ha acostumbrado a vivir así.

En el caso de los virus, todos aceptan los riesgos que quedan aunque se mantenga actualizado su antivirus y esté funcionando, pues consideran que es un riesgo que no va a desaparecer totalmente y sólo lo pueden mitigar.

En cuanto a la falta de suministro eléctrico, este tipo de eventos al tener una concurrencia mínima tienen un riesgo residual de igual tamaño

5.3.7. CONTROLES ADICIONALES

Después de analizar lo referido a los riesgos en este departamento se crearon algunas recomendaciones para disminuir sus vulnerabilidades y así los ataques causen un valor mínimo de impacto:

- Se recomienda en los laboratorios colocar bitácoras de acceso y restringir el acceso con credencial y en horarios de clases con un profesor a cargo.
- Se recomienda rediseñar el laboratorio de maquinas eléctricas así como sus oficinas para crear nuevas rutas de evacuación que realmente sean efectivas.
- Realizar un estudio sobre los efectos negativos en personas de la subestación.
- Colocar cámaras de video en puntos estratégicos para evitar así el robo de equipos de cómputo.
- Crear un manual de buenas prácticas para el uso de equipos de cómputo (que incluya antivirus y claves de acceso), así como darle gran difusión.
- En el laboratorio de Eléctrica de Potencia, realizar un estudio sobre los niveles de confianza de todos los equipos para garantizar su alta disponibilidad.
- En el mismo laboratorio, colocar mecanismos de control de acceso a estudiantes y administradores para el uso correcto de los equipos de cómputo.

5.4 DEPARTAMENTO DE ELECTRÓNICA[18]

El análisis de riesgo aplicado a este departamento se limitó al área de oficinas del Departamento de Ingeniería Electrónica. Este departamento cuenta con un servidor web el cual contiene información del área y switches, los cuales son administrados por el encargado de la red.

[18] Véanse los cuestionarios en el apéndice D y en el apéndice E las estadísticas y el análisis de resultados

Se utiliza el mecanismo NAT[19](Network Address Translation- Traducción de direcciones de red) para el otorgamiento de direcciones virtuales IP y el servicio de Internet.

5.4.1. IDENTIFICACIÓN DE ACTIVOS

Se pueden observar los siguientes activos:

I. Equipo de Cómputo: computadoras de oficina, computadoras de laboratorio, computadoras de desarrollo, servidor, switches, impresoras, escáners, laptops.

II. Equipo de instrumentación: Multímetros, osciloscopios ,analizadores de espectros, fuentes de voltaje, amperímetros, generadores de señales.

III. Documentación: Calificaciones, libros, oficios, manuales, trabajos de investigación.

5.4.2. IDENTIFICACIÓN DE AMENAZAS

En la tabla 5.3 se muestran las amenazas identificadas en el departamento:

Tabla 5.3 Amenazas identificadas

Tipo de Amenaza	Descripción de Amenaza	Impacto	Frecuencia de Ocurrencia	Prioridad
Humana	1. Alguna persona puede entrar fácilmente al departamento y robar algún equipo de cómputo o equipo de instrumentación del laboratorio.	1. Provoca la pérdida del activo.	1. En cualquier momento.	Alta
	2. Se provoque un incendio por fumar en área laboral.	2. Pérdidas de bienes y documentos importantes y posibles daños a la salud.	2. En cualquier momento.	Baja
	3. Una persona dañe	3. Pérdida de la	3. En cualquier momento.	Alta

[19] Mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

	las instalaciones telefónicas. 4. Desconocimiento del número de personas que ha accedido a los laboratorios. .	comunicación 4. Robo de recursos del laboratorio sin saber quién es el responsable.	4. En cualquier momento.	Alta
Problemas de tipo lógico	1. Cualquier persona puede acceder a una computadora que no tenga clave,	1. Puede existir modificación, robo de información.	1. En cualquier momento.	Alta
Errores de Hardware	1. Una descarga eléctrica puede dañar el equipo de cómputo. 2. Que haya un corte de energía y se pierda la información no guardada. 3. El mal funcionamiento de la computadora por la antigüedad de la misma	1. Pérdida de información. 2. Pérdida de información y deficiencias en el funcionamiento de la computadora. 3. Perder los servicios a los cuales está destinada la máquina	1. En cualquier momento.	Baja Alta Alta
Errores de la Red	1. El corte de un cable expuesto o manipulación de éste mismo. 2. Se caiga la red o tenga problemas por	1. Afectaría la disponibilidad de los servicios de la red. 2. Problemas de acceso y falta de	1. En cualquier momento. 2. En cualquier	Alta Alta

	falta de capacidad.	recurso de la red.	momento.	
Natural	1. La lluvia dañe el cableado del equipo.	1. Causa daños por tal motivo deja de funcionar.	1. Cada vez que llueve.	Alta

5.4.3. IDENTIFICACIÓN DE VULNERABILIDADES

En la tabla 5.4 se muestran las vulnerabilidades identificadas en el departamento y se encuentran clasificadas por tipo:

Tabla 5.4 Vulnerabilidades identificadas

Vulnerabilidades	
Física	Los equipos no cuentan con una contraseña para acceder a ellos. El acceso al laboratorio abierto no está controlado de manera eficaz, cualquier persona tiene acceso a él y al material que ahí se encuentra.
Hardware	Ninguno de los equipos, ni siquiera el NAT, cuenta con un no-break para prevenir la pérdida de información debida a fallas del suministro de la energía eléctrica
Red	Existen fallas en el cableado estructurado en el tendido del cable. La denegación de servicio puede ocasionar varios problemas, uno de ellos es la pérdida de comunicación entre los laboratorios del departamento que sirven para evitar contingencias.
Naturales	No se cuenta con un plan de contingencia en caso de incendio, además que muchos de los activos son los libros y no se tiene manera de recuperarlos en caso de pérdida.
Humana	No se cuentan con políticas de seguridad sólo con “acuerdos” y se desconocen las políticas de seguridad en la institución.

5.4.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

En la actualidad sólo se ha presentado la denegación de servicio, lo cual ocasionó que se perdiera la comunicación entre los laboratorios del departamento y de esta manera la pérdida temporal de los servicios.

Hasta ahora, como el acceso al laboratorio abierto no está controlado de manera eficaz, cualquier persona tiene acceso a él y al material que ahí se encuentra, el cual ha sufrido pérdidas.

5.4.5. CONTROLES EXISTENTES

La tabla 5.5 muestra los controles existentes en el departamento.

Tabla 5.5 Controles existentes

Controles requeridos	Descripción	Controles discrecionales	Descripción
Control de acceso	• Se cuenta con una puerta de acceso a la división y a cada cubículo. • El acceso al laboratorio de instrumentación es restringido.	Horario de acceso y control de acceso.	• Se maneja un horario de 7 AM a 9 PM en el que está abierta la puerta de acceso al departamento “puerta de cristal”, excepto a la hora de la comida 2 PM a 3 PM donde permanece cerrada. • La llave de los cubículos sólo la tiene cada responsable del cubículo y la secretaria.
Acceso al laboratorio abierto	• El alumno que ingrese debe autenticarse como tal.	Control de acceso.	• El alumno deja al encargado del laboratorio su credencial de estudiante para ingresar a éste.
Soporte	• Los usuarios deben acudir con el responsable de soporte técnico en caso de tener algún problema con el equipo.	Encargado del soporte.	• En caso de detectar algún virus o problemas con el equipo, los usuarios solicitan el apoyo del ingeniero encargado del soporte técnico.
Acceso al laboratorio de sistemas	• El acceso es restringido.	Acceso a	• Sólo se puede acceder a los laboratorios en horario de clase y con el profesor

embebidos y a los laboratorios de electrónica		laboratorios.	responsable presente.
NAT	• Asigna IP virtuales a los equipos de la red disminuyendo la posibilidad de un ataque externo.	Sistema	• No abrir correos de remitentes desconocidos.

5.4.6. RIESGOS RESIDUALES

En la tabla 5.6 se muestran los riesgos residuales.

Tabla 5.6 Riesgos residuales

Riesgo	Control no existente
Pérdida de información.	Algunos equipos de cómputo no cuentan con contraseñas.
Robo de instrumental del laboratorio.	Al no existir un control adecuado de las personas que acceden a los laboratorios, así mismo del los instrumentos pequeños, existen pérdidas de material pequeño y fácil de ocultar.
Deficiencias en el cableado estructurado.	Algunos cables se encuentran en mal estado, esto dificulta el buen funcionamiento de la red dentro del departamento.
No existen planes de contingencia	Ante alguna emergencia debería de diseñarse algún plan de contingencia para salvaguardar los activos del departamento.

5.4.7. CONTROLES ADICIONALES

En la tabla 5.7 se muestran los controles que se recomiendan para el departamento.

Tabla 5.7 Controles adicionales

Recomendaciones controles requeridos	Descripción	Recomendaciones controles discrecionales	Descripción
Autenticación	• Todos los equipos deberán contar con una contraseña de 6 dígitos	Autenticación	• La contraseña debería ser sugerida por el administrador y poder ser modificada por el usuario, pero

	que incluya mayúsculas minúsculas, números y caracteres especiales.		el sistema debe validar que sea una contraseña segura.
Control de acceso al laboratorio abierto	• Todo alumno que ingrese deberá ser registrado en una base de datos que contenga la información del alumno y el equipo que está utilizando.	Control de acceso al laboratorio abierto.	• No debería haber más de 4 alumnos por mesa de trabajo.
Control de acceso al departamento	• Debe llevarse un registro de las personas que accedan, registrando tanto su hora de entrada como la de salida.	Control de acceso al departamento	• Deberán dejar una identificación oficial al entrar y recogerla al salir
Equipo	• Todo equipo de cómputo debe contar con no-break.	Equipo	• Se deben guardar cada 5 minutos los documentos en los que se esté trabajando
Cableado estructurado	• Corregir fallas del cableado estructurado	Cableado estructurado	• Se debe revisar y corregir cada 6 meses el cableado estructurado
Prevención de incendios	• Plan de contingencia	Prevención de incendios	• Contar con un extinguidor por cubículo

5.5 DEPARTAMENTO DE PROCESAMIENTO DE SEÑALES[20]

Dentro del Departamento de Procesamiento de Señales, se tienen 5 laboratorios donde se cuenta con diferentes equipos y usos, la cantidad de los activos también difiere, así como los servicios que brinda, el acceso a los mismos se realiza con base en las normas o recomendaciones realizadas por cada responsable del laboratorio.

A continuación se presenta un análisis de cada laboratorio teniendo en cuenta sus valores, vulnerabilidades, las amenazas y el impacto que generan si dejan de dar servicio.

Los laboratorios con los que se cuenta en este departamento son:

a) Laboratorio de procesamiento digital de imágenes

Las principales actividades del laboratorio es la de proporcionar servicios a los alumnos.

b) Laboratorio de procesamiento de voz

Las principales actividades están relacionadas al procesamiento de voz, investigaciones realizadas por tesistas y prácticas de laboratorio de licenciatura y maestría.

c) Laboratorio de procesamiento digital de imágenes (2)

Se realizan actividades de investigación en el área de Procesamiento Digital de Imágenes Cada computadora personal se encuentra asignada a un usuario del laboratorio, por medio de los equipos se desarrollan los algoritmos usados en el procesamiento de las imágenes. El equipo servidor administra determinados servicios a los que tienen acceso los equipos de cómputo para su adecuado funcionamiento.

d) Laboratorio de procesamiento digital de señales

Las principales actividades son: Docencia de posgrado y materias de la licenciatura, alumnos de servicio social, tesis de licenciatura y maestría.

e) Laboratorios de análisis, calidad y seguridad de la información

Las principales actividades son las realizadas por los alumnos de posgrado y docencia.

[20] Véanse los cuestionarios en el apéndice D y en el apéndice E las estadísticas y el análisis de resultados

La mayoría de los profesores de este departamento laboran en otro edificio de la licenciatura o en salones de posgrado, el área cuenta con cubículos para alumnos de posgrado, otros para los de control (licenciatura y posgrado) y procesamiento de señales (posgrado). Cada profesor tiene a su cargo su laboratorio a veces junto con otro profesor.
Se sabe que existen políticas de seguridad pero no se consideran relevantes comparadas con las problemáticas de infraestructura del edificio.

5.5.1. IDENTIFICACIÓN DE ACTIVOS

El departamento está compuesto por laboratorios en los cuales se encontraron los siguientes activos:

a) Laboratorio de procesamiento digital de imágenes

El laboratorio cuenta con un servidor y varias computadoras, de las cuales no se especifica el número y tampoco se tiene un estimado del valor de los activos con los que cuenta el laboratorio.

b) Laboratorio de procesamiento de voz

Sus principales activos con los que cuenta y brinda sus servicios son: multímetros, osciloscopios, generadores de señales, fuentes de energía y de prueba DSP, cuentan con equipo de cómputo básico.
No se tiene un valor estimado de los activos.

c) Laboratorio de procesamiento digital de imágenes (2)

Este laboratorio cuenta con lo siguiente: 8 computadoras personales, un equipo servidor, 4 estaciones de trabajo, 2 impresoras láser, 1 concentrador (hub), 1 enrutador WI-FI, 1 switch Ethernet, 1 cámara se seguridad inalámbrica, 10 UPS (sistema de alimentación ininterrumpida), algunos de los equipos cuentan con bases de datos de imágenes y algoritmos para el procesamiento de las mismas (información),

Donde el servidor, las 8 computadoras, el enrutador y el switch son catalogados como lo más importante.

d) Laboratorio de procesamiento digital de señales

El laboratorio cuenta con lo siguiente: Mesas, sillas, equipos de cómputo, generadores, osciloscopios, tarjetas con cámara, tarjetas para aplicaciones de voz y video.

e) Laboratorios de análisis, calidad y seguridad de la información

Cuenta con el siguiente equipo: Computadoras, robots, equipos de laboratorio de comunicaciones y electrónico (VNA, analizadores de espectro, osciloscopios, cámaras, equipos de audio, equipo de redes, pizarrones electrónicos, cañones de proyección, copiadoras, etcétera), 2 Servidores (Verona y Pacific), 1 Servidor Dell descompuesto en espera de reparación, equipos de red

Lo más importante para este departamento son los servidores (Verona, Pacific) y los equipos de red (routers), además de un osciloscopio.

5.5.2. IDENTIFICACIÓN DE AMENAZAS

a) Laboratorio de procesamiento digital de imágenes

En este laboratorio la mayor amenaza es la desconfiguración de los equipos de cómputo ya que se deja de dar servicio en ese equipo lo cual conlleva a la denegación de servicio, sucede muy frecuentemente.

b) Laboratorio de procesamiento de voz.

En este laboratorio una amenaza son los virus informáticos, éstos presentan denegación del servicio aproximadamente de un día, lo cual sucede no muy frecuentemente.

El robo de equipo es otro problema, esto conlleva a la denegación del servicio, además de no brindar los servicios adecuadamente o en forma.

c) Laboratorio de procesamiento digital de imágenes (2)

En este laboratorio las principales amenazas son:

- Fallas en el suministro de corriente que pueden dañar a los equipos, se presenta muy frecuentemente.
- El calor extremo de algunos meses del año.
- Daño de las fuentes de alimentación, discos duros, unidades ópticas y fallas en los sistemas de enfriamiento. Sucede no muy frecuentemente.

Todas las fallas que se presentan en este laboratorio conllevan a la denegación del servicio el cual podría durar hasta que la falla se haya canalizado al área correspondiente y se le haya dado solución.

d) Laboratorio de procesamiento digital de señales

Las principales amenazas en este laboratorio son las siguientes:

- Falla de la energía eléctrica o sobrecargas.
- El mal uso de las tarjetas al conectar una interfaz
- Que alguna de las tarjetas se caiga o se golpee.

e) Laboratorios de análisis, calidad y seguridad de la información

Las principales amenazas en este laboratorio son:

- Robo de equipo. El personal no sabe cómo actuar ante esta situación.
- La distribución de los edificios y mobiliarios.
- Pésimo diseño de las escaleras y barandales.
- Se descartan los daños ocasionados por desastres naturales tales como temblores.
- Puerta de acceso del pasillo descompuesta.

Los robos han ocurrido durante el día, sin violencia y cuando el edificio está solo, no se especifica la frecuencia de los robos.

5.5.3. IDENTIFICACIÓN DE VULNERABILIDADES

a) Laboratorio de procesamiento digital de imágenes

- No se conocen las políticas de seguridad.
- No se realizan evaluaciones para determinar el nivel de conocimiento de las personas que laboran en el laboratorio.
- Para el control de acceso se cuenta únicamente con un candado y cadena.

b) Laboratorio de procesamiento de voz

- No se conocen las políticas de seguridad.
- No se sabe la correcta operación de los equipos.
- No se cuenta con antivirus instalado y actualizado.
- No contar con medidas de seguridad más robustas como candados o chapas para evitar el robo de equipo.
- Filtraciones de agua en las instalaciones lo cual puede provocar corto circuito y eventuales daños.

c) Laboratorio de procesamiento digital de imágenes (2)

- Aunque se cuenta con los UPS, éstos no están siendo utilizados.
- No se tiene un sistema de aire acondicionado.

d) Laboratorio de procesamiento digital de señales

- No se conocen las políticas de seguridad.
- El número de tarjetas es limitado
- No cuentan con seguros ni con protecciones mayores.

e) Laboratorios de análisis, calidad y seguridad de la información

- No hay capacitación para los vigilantes.
- No hay mantenimiento para la instalación eléctrica.
- No hay rampas de emergencia.
- No hay mantenimiento del elevador.
- No hay buena seguridad, cadenas y candados de mala calidad.
- No hay UPS para cuidar equipos por sobretensiones.
- La red y el equipo de red no están actualizados.
- No cierran la puerta del laboratorio abierto (frecuentemente).
- No hay control de acceso, puede pasar cualquier persona

5.5.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

a) Laboratorio de procesamiento digital de imágenes

El impacto principal es la denegación de servicios, lo cual es la actividad principal del laboratorio.

b) Laboratorio de procesamiento de voz

En general las consecuencias serían de tipo económico porque se cuenta con equipo por duplicado para la mayoría de las actividades así como también se respalda frecuentemente la información contenida en el equipo de cómputo.

c) Laboratorio de procesamiento digital de imágenes (2)

En el caso de pérdida o daño de un equipo, se le asigna otro de manera temporal al usuario afectado, el cual tendrá que compartir con el usuario del equipo asignado.

El usuario asignado al equipo quedaría sin la posibilidad de continuar con el desarrollo de los algoritmos propios de su investigación y se perdería el avance inmediato de dicha investigación así como un retraso en su calendario de actividades.

d) Laboratorio de procesamiento digital de señales

- Si se daña alguna tarjeta se quedaría detenida la investigación.

e) Laboratorios de análisis, calidad y seguridad de la información

- Si se pierde el servidor Pacific o los equipos de red, muchos miembros del personal no podrían conectarse a internet.
- Si se pierde el servidor Verona, no habría correo ni página para los aspirantes a posgrado ni para el departamento en general.

5.5.5. CONTROLES EXISTENTES

a) Laboratorio de procesamiento digital de imágenes

En este laboratorio, no se tiene implementado ningún control de acceso como tal, sólo se cuenta con una cadena y un candado para el resguardo de los activos. Aunque se está implementando un sistema de seguridad con alarmas.

b) Laboratorio de procesamiento de voz

En horario laboral, el laboratorio se encuentra vigilado por un encargado. Si los alumnos quieren ingresar al laboratorio, es necesario que sean acompañados por un profesor.
Los tesistas y personal autorizado cuentan con llave del laboratorio que les es proporcionada por el encargado.

c) Laboratorio de procesamiento digital de imágenes (2)

I. Controles requeridos

En el laboratorio se cuenta con la siguiente seguridad en el laboratorio:

- Una alarma. La cual se activa cada vez que el laboratorio se desocupa y sólo los usuarios del laboratorio conocen cómo desactivarla.
- Una cámara de vigilancia. La cual puede consultarse en forma remota y en cualquier momento, así como revisar los videos anteriores.
- En el caso de la alarma, todos los usuarios son responsables de activar y desactivar la alarma. La vigilancia remota es llevada a cabo por parte del administrador del laboratorio así como del investigador responsable.
- Sólo el usuario puede tener acceso a su equipo asignado.
- Existe una relación interna de los números de inventario de los bienes.

II. Controles discrecionales

A manera de prevención se hace lo siguiente:

- Revisión de posibles programas espías instalados o modificación del sistema operativo.
- Reemplazar la información modificada por el último respaldo realizado.
- Modificar la contraseña y revisar la robustez de la misma.
- Como medidas precautorias se realizan respaldos periódicos, la instalación de programas anti-espía y la revisión constante de los videos de seguridad.

d) Laboratorio de Procesamiento Digital de Señales

- No se tiene implementado ningún control de acceso como tal

- ❖ Sólo se tiene una llave para controlar la entrada
- ❖ Para una tarjeta que existe en el laboratorio se tiene una cadena

e) Laboratorios de análisis, calidad y seguridad de la información

I. Controles requeridos

- ❖ Cerrar algunas puertas
- ❖ Usar cadenas

II. Controles discrecionales

- ❖ La implementación de un sistema de alarma el cual ahuyentó a un ladrón.
- ❖ Los vigilantes de la noche revisan que estén cerradas las puertas tirando de la manija.
- ❖ La implementación de un firewall que cubre a todos los que están en el segmento de red del departamento.
- ❖ El uso de correo electrónico por el puerto 80.

5.5.6. RIESGOS RESIDUALES

a) Laboratorio de procesamiento digital de imágenes

Para el caso de la desconfiguración de equipo es necesario que los usuarios accedan sin derechos de administración. Que de igual manera no se tiene un impacto si se realiza una buena administración de los equipos, otorgando privilegios a los administradores y sólo a ellos.

b) Laboratorio de procesamiento de voz

Con respecto a los antivirus, la correcta instalación y actualización de los mismos proporcionaría una mayor seguridad, así como las instalaciones de una chapa o mejores sistemas de seguridad para la protección de lo activos.

c) Laboratorio de procesamiento digital de imágenes (2)

En el caso del suministro eléctrico, se cuenta con UPS, la conexión de los equipos a sus respectivos UPS sería de mucha utilidad, además la de prevenir que los equipos se apaguen de manera errónea y proteger sus componentes como discos duros, fuentes de alimentación.

La instalación de un sistema de aire acondicionado mejoraría notablemente el ambiente en donde se encuentran los equipos ya que de lo contrario el sobrecalentamiento puede afectar notablemente los equipos.

d) Laboratorio de Procesamiento Digital de Señales

Debido a que las tarjetas son el activo más preciado sería necesario realizar lo siguiente:

- Sólo personal calificado podría hacer uso de las tarjetas.
- Si se trata de alumnos, éstos deben ser supervisados.
- Colocación de extinguidores en el laboratorio.

e) Laboratorios de análisis, calidad y seguridad de la información

Con la información recabada en este departamento se puede concluir que el diseño de los cubículos para los profesores y los laboratorios están mal diseñados, estratégicamente hablando, ya que cualquier persona tiene acceso a cualquier parte del edificio, el control de acceso es un problema grave en esta área pues hasta robos se han presentado, la falta de capacitación y supervisión de los vigilantes es un factor crítico, en última instancia y no por eso menos riesgosa, es el mal estado en general del edificio.

5.5.7. CONTROLES ADICIONALES

a) Laboratorio de Procesamiento Digital De Imágenes

I. Controles requeridos

- Investigación, conocimiento y difusión de las políticas de seguridad de cómputo.
- Asignar sesiones de usuario para que no se haga uso indebido del equipo de cómputo.
- Utilizar contraseñas robustas y con caracteres alfanuméricos.
- Realizar un inventario de los bienes en el laboratorio.

- Capacitación del personal que ingrese al laboratorio respecto a las políticas de seguridad de cómputo.
- Utilización de antivirus para el servidor que pueda dar servicio a las estaciones de trabajo.
- Uso de un firewall.
- Hacer uso de programas antispyware.
- Evaluar los conocimientos del asistente del equipo de cómputo para saber si se está lo suficientemente preparado para enfrentar amenazas inesperadas.

II. Control Discrecional

- Colocar una cámara de vigilancia.

b) Laboratorio de procesamiento de voz

I. Controles requeridos

- Colocación de chapas especiales (electrónicas) o candados en el lugar ya que se aceptó que una amenaza probable es el robo de equipo.
- Actualización periódica de un antivirus, es recomendable adquirir uno para el servidor, así se tendrá protección para cada estación de trabajo.
- Hacer uso de un firewall.
- Hacer uso de programas antispyware.
- Realizar un inventario del equipo.
- Cambiar las contraseñas de inicio de sesión constantemente.
- Conocer y difundir las políticas de seguridad.

c) Laboratorio de Procesamiento Digital de Imágenes (2)

I. Controles requeridos

- Capacitación continua del personal.
- Investigación, conocimiento y difusión de las políticas de seguridad de cómputo.

II. Controles discrecionales

- Debido a que el laboratorio tiene su mayor activo en los equipos de cómputo, aplicar el uso de cerraduras más sofisticadas.

d) Laboratorio de Procesamiento Digital de Señales

I. Controles requeridos

- Investigación, conocimiento y difusión de las políticas de seguridad de cómputo.
- Colocación de chapas especiales (electrónicas) o candados.
- Gabinetes especiales para el resguardo de las tarjetas.

II. Control discrecional

- Colocar una cámara de vigilancia.

e) Laboratorios de análisis, calidad y seguridad de la información

I. Controles requeridos

- El buen funcionamiento de las puertas de acceso.
- Mantenimiento en general de todas las áreas.
- Se recomienda redistribución de cubículos, laboratorios y áreas de investigación.
- Un control de acceso, registrar a las personas que salen y entran del área, los trabajadores deberán identificarse.
- Capacitación continúa para los vigilantes.
- Presencia de vigilante permanente en ciertas áreas como las áreas de investigación.
- Los equipos electrónicos deben tener reguladores.

II. Controles discrecionales

- Cerciorarse que la puerta esté bien cerrada.
- Incluir una cerradura extra

- Hacer respaldos de información

.

- Evitar dejar cosas de valor personales en el cubículo, en la medida de lo posible.

5.6 DEPARTAMENTO DE SISTEMAS ENERGÉTICOS[21]

En este departamento se observa lo siguiente:

a) Cubículo de Sistemas Energéticos

- Se cuenta con un servidor que está ubicado en uno de los cubículos.
- Dentro del departamento se cuenta con un punto de acceso para brindar el servicio de red inalámbrica. La forma en la que se configuró el punto de acceso es de la siguiente manera: cifrado, filtrado por MAC y Autenticación WEP.
- Los equipos que se conectan a la red son aproximadamente de 23 a 25.
- Los dispositivos con los que se cuenta son los siguientes: 2 switches, un hub y un router con capacidad Inalámbrica y además un servidor con dos tarjetas de red, un procesador XEON, teclado, monitor, ratón, Windows Server 2003, Norton, Unidad Combo y Unidad 3 ½.
- El administrador del servidor es el encargado de habilitar y deshabilitar los puertos. Se tienen activos los puertos para acceso a Internet y el de acceso remoto está deshabilitado debido a que no es necesario ese servicio.

b) Laboratorio de Sistemas Energéticos ubicado en la planta baja

- Están conectados a una red local.
- No se cuenta con redes inalámbricas.
- El sistema operativo que administra la red está actualizado y debidamente configurado.
- Se cuenta con dos servidores. (Uno es un servidor de correo y página web y el otro es para almacenar proyectos).

c) Laboratorio de Sistemas Energéticos ubicado en el primer piso

[21] Véanse los cuestionarios en el apéndice D y en el apéndice E las estadísticas y el análisis de resultados

- El laboratorio está conectado a una red local.
- Tienen acceso a Internet.
- No se cuenta con red inalámbrica
- Se tiene un servidor de impresión.
- No han tenido problemas con la configuración del sistema en la red.

5.6.1. IDENTIFICACIÓN DE ACTIVOS

a) Cubículo de Sistemas Energéticos

Los activos son los equipos de cómputo y las características físicas que los hace diferentes a las demás computadoras y la paquetería que requiere el usuario puede variar dependiendo del trabajo que se esté realizando.

Se cuenta con paquetería que se administra en los equipos de cómputo ésta contempla: office profesional, Norton Internet Security, Windows XP Home y Professional, McAfee 2006.

Los activos importantes son los documentos de word, excel y planos de AUTOCAD que se administran en el departamento. Se tienen 23 equipos, un servidor que está ubicado en uno de los cubículos,un punto de acceso, 2 switches, un hub y un router .

b) Laboratorio de Sistemas Energéticos ubicado en la planta baja

- Se trabaja en el laboratorio con software especializado y modelos del mismo.
- Cuentan con equipos para el servicio de impresión.
- Cuentan con 9 equipos de cómputo de distintas características.

Los activos son de gran utilidad para los usuarios, por lo que necesitan estar protegidos para realizar sus trabajos y manejar su información de manera cuidadosa.

c) Laboratorio de Sistemas Energéticos ubicado en el primer piso

- Se tiene inventario de los equipos y dispositivos externos.

- El laboratorio cuenta con 6 equipos Pentium 4 a 2.4GHz, 120GB en DD y 512MB en RAM.

5.6.2. IDENTIFICACIÓN DE AMENAZAS

a) Cubículo de Sistemas Energéticos

- Robo de equipos
- Fallas eléctricas que pueden derivar en incendios

b) Laboratorio de Sistemas Energéticos ubicado en la planta baja

- Si se va la luz no se puede trabajar.
- Denegación de servicios.
- Infección de equipos por virus informáticos.

c) Laboratorio de Sistemas Energéticos ubicado en el primer piso

- El software sin licencia está expuesto pues no se puede actualizar, esto afectar el sistema.
- Pérdida de información sin forma de recuperarla.
- Daño físico de los equipos al realizar limpieza y mantenimiento
- Robo de equipo.
- Denegación de servicios sin previo aviso.
- Infección de equipos por virus.

5.6.3. IDENTIFICACIÓN DE VULNERABILIDADES

a) Cubículo de Sistemas Energéticos

- Se cuenta con políticas de seguridad pero hay desconocimiento por parte de los usuarios y también del personal administrativo.
- El departamento no cuenta con extinguidores
- El departamento no cuenta con mecanismos de seguridad que pueden ser cámaras de video, alarmas y etcétera.

- En las instalaciones que tiene el departamento, no hay aire acondicionado ni ventilación.

b) Laboratorio de Sistemas Energéticos ubicado en la planta baja

- No cuentan con políticas de seguridad.
- No tienen comunicación con otros departamentos.
- No cuentan con extinguidores.
- No hay un sistema de registro de los usuarios.
- En caso de que haya fallas de hardware se reportan a mantenimiento y si se presenta un mal funcionamiento debido al software, el tesista se hace cargo de la máquina.
- El mantenimiento al centro de cómputo es por solicitud.
- No cuentan con ventilación.
- No hay responsables de recoger los respaldos. Se tienen copias en distintos lugares.
- No hay botiquín de primeros auxilios.

c) Laboratorio de Sistemas Energéticos ubicado en el primer piso

- Sólo el sistema operativo cuenta con licencia.
- No hay copias de seguridad de los programas.
- El cableado en general está en desorden.
- No se cuenta con un plan de contingencia.
- No hay alguien presente cuando se hace la limpieza.
- No se cuenta con extinguidores en el área de trabajo en caso de un incendio.
- Puede entrar un usuario que no sea del departamento de sistemas energéticos siempre y cuando tenga autorización de la secretaria o del jefe del Departamento.
- No existe un sistema de administración de red como tal, ya que la restricción se hace localmente.

- No se cuenta con botiquín de primeros auxilios

5.6.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

- Si se llegara a presentar alguna falla en los equipos de cómputo, se revisa el sistema o son enviados a los encargados del mantenimiento de la institución, presentándose estas fallas cada 3 o 6 meses.

- Para que el usuario pueda acceder al servicio de red debe pedirle permiso a los administradores para poder realizar su trabajo. Si se presenta la negación de los servicios de red a todos los departamentos, se perjudica a todos los usuarios y al personal administrativo.

- El impacto que tendría la pérdida de información no lo toman en cuenta, según se comentó, pues es información especializada y sólo puede ser interpretada por personas con grado de maestría o doctorado en el área.

5.6.5. CONTROLES EXISTENTES

a) Cubículo de Sistemas Energéticos

- Los empleados o encargados que pertenecen al departamento se enteran de los avisos emitidos por la institución.

- Se realiza la limpieza de los equipos de cómputo y de red así como de los cubículos bajo supervisión de los jefes o encargados en turno.

- El mantenimiento de los equipos de cómputo se realiza cada 6 meses, lo más conveniente se aplica al término del semestre o ciclo escolar.

- Todos los equipos de cómputo cuentan con software original de cualquier paquetería que se usa en ese departamento

- Se realiza una revisión semanal al servidor para saber el estado general del equipo y cada 15 días se efectúa un respaldo de la información para evitar su pérdida.

- El administrador tiene registrado a todos los usuarios en su sistema de cómputo y para darlos de alta deben trabajar en el departamento.

- Los permisos para los usuarios externos que no pertenecen al departamento son otorgados por los responsables de los proyectos que se estén desarrollando.

- Los usuarios no pueden descargar información que no esté relacionada con su trabajo ni pueden instalar programas.

- El departamento cuenta con una lista de todos los usuarios internos y externos, dicha lista está a cargo del administrador, las secretarias y el propio responsable del departamento.

- El administrador del servidor es el encargado de habilitar y deshabilitar los puertos que son los más empleados, por spyware o troyanos, se tienen activos los puertos para acceso a Internet y el de acceso remoto está deshabilitado debido a que no es necesario ese servicio.

- Se realizan por lo menos dos respaldos universales para evitar pérdida de información en el departamento

- En el horario de comida se quedan en guardia las secretarias de los encargados del proyecto

- Los equipos de cómputo cuentan con un firewall a nivel de software que se encuentra actualizado.

- El sistema operativo que administra la red está actualizado y debidamente configurado.

- Los mecanismos de seguridad que implementa el servidor son los siguientes: contraseña mayor a 7 caracteres, se tiene determinado quién puede entrar a qué directorio y se cuenta con Norton para supervisar el acceso desde Internet.

b) Laboratorio localizado en la planta baja

- Cuenta con información impresa, respaldos de información y en caso de pérdida de ésta, se puede obtener de las fuentes originales.

- Siguen el plan de contingencias de Posgrado.

- Cuentan con no-break.

- La limpieza es supervisada.

- No se permite descargar software, videos ni música.

- Todos los equipos cuentan con licencias de software.

- A la hora de la comida se cierra el o los laboratorios.

- Para tener acceso a las computadoras del laboratorio se necesita ser tesista del departamento de sistemas energéticos.

c) Laboratorio de Sistemas Energéticos ubicado en el primer piso

- Se hace respaldos de la información sólo si los profesores lo solicitan y se ponen nuevamente en el equipo que utilizan.
- La frecuencia con que se hace un análisis a las computadoras es cada 2 o 3 meses.
- Para tener acceso a las computadoras del laboratorio se necesita ser alumnos de posgrado y anotarse en una libreta.
- El control de seguridad que usa es restringir a los usuarios.
- Se le da mantenimiento a todas las computadoras del laboratorio de Sistemas Energéticos cada 6 meses.
- Tienen no-break.
- No se permite descargar software, videos, música o instalar algún programa.
- Tienen ventilación o aire acondicionado en los laboratorios de cómputo.

5.6.6. RIESGOS RESIDUALES

a) Cubículo de Sistemas Energéticos

- No todos equipos de cómputo cuenta con energía regulada, solamente algunos equipos (el servidor y algunas máquinas) por lo que el daño a los equipos es latente.
- El cableado de red que tiene el departamento, no está bien organizado ni se puede identificar; si se presenta una contingencia, puede haber problemas sobre el cableado que se hizo para dar el servicio de Internet. El cableado de red no se encuentra sobre un soporte o una estructura de canaletas de plástico que le brinden protección contra vibraciones de ruido, polvo, campos magnéticos y etcétera.

b) Laboratorios localizados en la planta baja y primer piso

- El riesgo de infección por virus es latente por el constante tráfico de información que los tesistas llevan a cabo.

- En caso de un incendio no se tienen extinguidores para apagarlo.

5.6.7. CONTROLES ADICIONALES

a) Cubículo de Sistemas Energéticos

Se hacen las siguientes recomendaciones para tener una organización en el cubículo:

- Se debe contar con algunos extinguidores contra incendios.
- Se debe contar con un dispositivo manual de emergencia para cortar el sistema eléctrico y el aire acondicionado deberá instalarse en cada salida de la sala de cómputo.
- Se debe tener un botiquín de primeros auxilios, para cualquier accidente.
- Se recomienda que se compre un UPS más grande para que pueda soportar el voltaje de todos los equipos de computo.

Se les recomienda que es indispensable que la alimentación a los equipos de cómputo sea mediante energía eléctrica regulada; para ello, y dependiendo de las condiciones, deberá considerarse:

- Primero: A través de un sistema de energía no interrumpible (equipo no-break con regulador de voltaje).
- Segundo: A través de un regulador de voltaje, el cual puede tener dispositivos que eliminen ciertas armónicas perjudiciales al equipo de cómputo.
- Tercero: Para equipos de cómputo pequeños del tipo computadora personal a través de un multicontacto que permita eliminar armónicas y conectado a un regulador de voltaje individual o de mayor capacidad o conectado a un equipo no-break con regulador de voltaje.
- Espacio para el equipo de aire acondicionado

b) Laboratorios localizados en la planta baja y primer piso

- Se debe tener el reglamento del laboratorio disponible para los usuarios y a la vista.
- Se debería tener un sistema de registro de los usuarios.

- Se debe tener en orden a los equipos y a los cables para no provocar un accidente.

- Se debe tener conocimiento de las políticas de seguridad para poder tener un mejor manejo y utilización de las redes evitando así la negación de los servicios.

- Debe existir un lugar donde se organice la información que se va respaldando.

5.7 DEPARTAMENTO DE TELECOMUNICACIONES[22]

El Departamento de Ingeniería en Telecomunicaciones se encuentra constituido por personal académico, personal de oficina, equipos de cómputo, equipos de laboratorio, muebles, laboratorios, cubículos y equipos electrónicos diversos.

Los laboratorios ubicados en este departamento son: Laboratorios de óptica, laboratorio de procesamiento de señales analógicas y digitales, laboratorio de electromagnetismo aplicado, laboratorio de sistemas de comunicaciones, laboratorio de comunicaciones digitales, laboratorio de videoconferencia y enlaces satelitales, área de proyectos y taller, laboratorio de telecomunicaciones ópticas, laboratorio de redes inalámbricas, laboratorio de telefonía y radiocomunicaciones, laboratorio de nanosatélites.

5.7.1. IDENTIFICACIÓN DE ACTIVOS

El personal del departamento de Telecomunicaciones, en su mayoría profesores, reconoce como activos propios: Los Instrumentos de medición de señales eléctricas y electromagnéticas, computadoras, software, impresoras, libros, claves de acceso remoto, información tanto digital como física (propiedad intelectual), calificaciones, apuntes, artículos.

Los activos pertenecientes al departamento únicamente son: computadoras, impresoras, equipo de laboratorio en general (generadores, osciloscopios, multímetros, antenas), copiadoras, ferretería, libros.

La importancia de los activos personales fue medida en costos económicos y de tiempo, debido al impacto que ocasionarían en caso de que dichos activos se perdieran, esto fue considerado entre el personal del departamento de la siguiente manera:

[22] Véanse los cuestionarios en el apéndice D

- En cuanto a los bienes que maneja cada profesor, en caso de sufrir alguna pérdida, no resulta relevante, por lo que el precio que se adjudica no resulta con un gran costo económico.

- El tiempo de recuperación resultaría tardado en caso de no tener respaldada la información, en cuanto al mobiliario, no sería costoso, sin embargo, el tiempo de recuperación sería prolongado.

Así mismo se realizó una estimación de la importancia de los activos pertenecientes únicamente al departamento costeando su pérdida tanto económica como en tiempo:

- En la mayoría de los casos si los activos tuvieran una pérdida total, las actividades se suspenderían hasta que el material fuera recuperado en su mayoría.

- La recuperación de la totalidad de los activos sería costosa

- El tiempo estimado de la recuperación de los bienes es de aproximadamente de 7 a 10 años, debido a que el proceso de adquisición de bienes de importación por parte de la institución es enormemente tardada y en ocasiones imposible.

5.7.2. IDENTIFICACIÓN DE AMENAZAS

Los principales problemas que se presentan o se han presentado en el departamento, los cuales pueden ocasionar pérdidas o daños son los siguientes: Cortes de energía eléctrica (cada 3 meses), sismos, robos (poco frecuentes), virus en equipos de cómputo (poco frecuentes), interrupciones en servicios de red (poco frecuentes), fallas en el equipo de cómputo (anualmente).

5.7.3. IDENTIFICACIÓN DE VULNERABILIDADES

Las principales causas o descuidos que provocan los problemas mencionados anteriormente, según el personal académico son los siguientes:

- Cortes de energía eléctrica debido a la sobre carga de las líneas eléctricas y al problema de regulación de la energía en el edificio, ya que varias personas mencionaron que existe una parte regulada y otra no, manifestándose en los distintos toma corrientes en el edifico.
- Cortes de energía eléctrica debido a que no se encuentra en funcionamiento la subestación que se está en construcción desde hace tiempo.

- Virus en equipos de cómputo debido a no tener antivirus previamente instalado.
- Robos debido a falta de precauciones y vigilancia.
- Robos debido a que la cámara de seguridad no funciona.
- Falta de planeación para la realización de simulacros en el departamento.

Las medias de protección con las que se cuentan en el departamento son regidas por el jefe del departamento y de la institución, aunque en diversos casos no se conocen por el personal que labora.

5.7.4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

Dependiendo del tipo de valor del activo que sufra el daño por medio de una amenaza será el impacto que éste tenga sobre el personal o directamente con el departamento entero. En algunos casos el personal mencionó que el impacto no sería importante debido a que el personal no cuenta con activos de gran valor.

Las áreas de impacto detectadas durante el proceso de este proyecto son mencionadas a continuación:

- **Revelación:** En caso de perder la confidencialidad en los activos sensibles (firma digital, exámenes, etcétera) del departamento, sería de cierta manera grave, aunque no reflejaría un gran impacto, debido a que el personal no cuenta con documentos personales dentro del área de trabajo.
- **Modificación:** En caso de sufrir una modificación o alteración en la información que maneja el personal académico, no reflejaría un gran impacto debido a que la mayoría cuenta con respaldos actualizados.
- **Destrucción:** Si se llegara a perder por completo la información, ya que ésta ha sido eliminada, su recuperación sería costosa en tiempo y económicamente, debido a que su recuperación tardaría aproximadamente un año.
- **Denegación de Servicio:** En caso de no contar con algún servicio como lo es Internet, correo electrónico, causaría~~n~~ un gran impacto ya que la mayoría utiliza el correo electrónico para comunicarse con sus alumnos e Internet ya que desde ahí recaban la mayoría de la información que manejan.

5.7.5. CONTROLES EXISTENTES

Los principales controles del lugar son los requeridos ya que no existe personal que imponga sus propios controles discrecionales, entre los más utilizados se encuentren los siguientes:

- Respaldos constantes manteniéndolos fuera de la oficina.
- Herramientas de seguridad para la red (antivirus).
- Empleo de contraseñas en la información de gran valor.
- Cerraduras.
- Firewall.
- Ninguno en determinados casos.

5.7.6. RIESGOS RESIDUALES

Existen ciertas áreas en donde el acceso es relativamente sencillo como es la entrada al departamento, ya que cuenta con una puerta de aluminio que consta de una sola chapa al igual que las puertas de los laboratorios y cuarto de servidores que al igual cuentan con una puerta de aluminio fácil de penetrar .

Otro factor importante, como se mencionó, es que en todo el piso existen dos tipos de energía eléctrica: una regulada y otra no regulada, esto les provoca problemas con la energía eléctrica en las áreas de trabajo ocasionando pérdidas de información en algunos casos de dispositivos electrónicos, así como las fallas de éstos.

Por otra lado se comentó que el diseño del edificio no fue creado para implementar la instalación de una red cableada, por lo que se realizó una improvisación de ésta, implementada por los alumnos de la carrera de Telecomunicaciones, la cual fue renovada recientemente por el administrador de la red y que posteriormente se tiene contemplado modificar para que la instalación utilice fibra óptica.

En el cuarto de servidores, no se cuenta con orden en el cableado de los dispositivos de red, lo cual puede provocar una caída y destrucción de los mismos. Además los servidores no tienen un sistema de respaldo adecuado ya que como se indicó, sólo contaban con un no-break que se había quemado.

El personal académico no conoce la ubicación de los extinguidores con los que cuenta el departamento y en caso de conocer su ubicación, no tienen la capacitación adecuada para su utilización.

En cuanto a la seguridad del departamento, no existen cámaras que monitoreen constantemente la entrada y salida de las personas que visitan el departamento, por lo que no se identifica a las personas que por algún motivo atenten contra los activos con los que se cuenta.

5.7.7. CONTROLES ADICIONALES

De acuerdo con la información recabada durante el desarrollo del análisis, es posible proporcionar las recomendaciones de los controles para evitar algunas de las vulnerabilidades detectadas en el proceso de análisis.

Recomendaciones de controles requeridos:

- Chapas seguras y puertas seguras de acuerdo con el material del que se encuentran elaboradas.
- Reforzar la vigilancia en general
- Imponer políticas de acuerdo con el acceso de personas en el departamento.
- Contar con un antivirus y firewall en cada computadora personal que se conecte a la red.
- Realizar una revisión de la instalación de la energía eléctrica.
- Uso de extinguidores visibles en cada área de trabajo.
- Cursos de protección civil.
- Contar con una contraseña robusta y que mantenga los parámetros de seguridad requeridos en su implementación, para protección de la información valiosa.

Recomendaciones de controles discrecionales:

- En caso de que la subestación se encuentre terminada, es recomendable su utilización para mejorar el suministro de energía eléctrica.
- Contar con no-break en cada equipo de trabajo.

CONCLUSIONES

CONCLUSIONES

El análisis de riesgos permite identificar los activos, es primordial poder identificar estos bienes que son valiosos para poder ver contra quién se van a proteger y de qué se van a proteger, además brindan información sobre vulnerabilidades, amenazas y todos los problemas que existen en una organización con el único fin de establecer medidas que logren un nivel de seguridad alto y desarrollar planes de contingencia, ya que en caso de un ataque, es necesario regresar a la actividad normal lo antes posible.

Como metodología de diagnóstico para poder establecer la exposición a los riesgos por parte de una organización, se recurre al análisis de riesgo.

Al realizar un análisis de riesgo a siete departamentos de una institución escolar de nivel superior para identificar las amenazas en los activos, así como sus vulnerabilidades, fue posible determinar de manera formal cada una de las recomendaciones para protegerlos de forma adecuada.

Con base en la información recabada, se identificaron cada uno de los activos de la institución además de la importancia que éstos tienen para los diversos departamentos así como para el personal que labora en ella y el impacto que tienen en las actividades cotidianas si llega a ocurrir una eventualidad que provoque una pérdida total o parcial de éstos.

Se sabe que la seguridad no existe al 100% por lo que se tiene que trabajar continuamente en ella para poder conseguir ser lo menos vulnerable posible, por lo que el análisis de riesgo no debe ser realizado en una ocasión. La seguridad es cíclica, se debe analizar, proteger, detectar y reaccionar continuamente para que los activos de la organización estén protegidos debidamente, por lo que el análisis de riesgos debe ser repetido posteriormente para detectar nuevas amenazas y vulnerabilidades y actuar adecuadamente ante ellas.

Se pudo observar durante el desarrollo de la tesis que en general, los laboratorios de los distintos departamentos, en su gran mayoría, no cuentan con mantenimiento preventivo de hardware y software, sólo se realizan actividades correctivas, por lo que los gastos son mayores. También, en la mayoría de los laboratorios no se difunden medidas de seguridad a los usuarios ya que no cuentan con carteles visibles o una difusión adecuada de reglas que deberían seguirse.

En cuanto a los recursos humanos de la institución, se pudo notar que la gran mayoría de la gente encargada de los laboratorios no tiene la noción de lo que es la seguridad informática, por lo que las medidas de seguridad implementadas no son las adecuadas o son bastante débiles. Lo anterior crea un segundo problema; los usuarios, los cuales al no encontrar reglas en los laboratorios no hacen el uso

adecuado de los equipos y del lugar, eso sin mencionar que también existen varios usuarios que no tienen conocimientos básicos de seguridad informática, lo anterior hace evidente la falta de capacitación de los recursos humanos con los que cuenta la organización. Todo en conjunto forma un círculo vicioso que termina afectando a la institución y que pone en riesgo a los activos de la misma.

El conseguir la información necesaria para la realización del análisis fue sencillo sólo cuando el personal de los diversos departamentos cooperaba, en ocasiones mínimas no se pudo contactar con algún encargado, lo cual ocasionó retrasos e impedimentos en la obtención de datos relevantes para continuar con el análisis del riesgo.

Gracias al estudio realizado se tiene una base para poder omitir, perfeccionar o desarrollar controles que colaboren a mejorar las actividades en la institución, así como a resguardar sus activos relevantes.

Este análisis sirve como iniciativa para que otras dependencias de la institución, así como otras organizaciones, realicen un análisis de riesgo en sus instalaciones, ya que éste, es un punto fundamental en la estructura de seguridad de una organización.

Es de vital importancia hacer notar que un análisis de riesgo debe desarrollarse continuamente y que la facilidad de llevarlo a cabo en menor tiempo recae en la disponibilidad y cooperación del personal para aportar información relevante y veraz que permita llegar a un punto concluyente, lamentablemente la falta de capacitación en el campo de la seguridad impide que el análisis de riesgo transcurra de manera fluida, pues actualmente la poca conciencia de algunas organizaciones sigue viendo a la seguridad de la información como un gasto y no como una inversión.

APÉNDICE A

Glosario

GLOSARIO

Activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Algoritmo Criptográfico: Un algoritmo criptográfico, o cifrador, es una función matemática usada en los procesos cifrado y descifrado. Un algoritmo criptográfico trabaja en combinación con una clave (un número, palabra, frase, o contraseña) para cifrar y descifrar datos.

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Atacante (perpetrador): Persona que se introduce a algún sistema sin tener acceso a él.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Clave de Cifrado: Una clave, llave, palabra clave, o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

Cliente/Servidor: Esta arquitectura consiste básicamente en un cliente que realiza peticiones a otro programa -el servidor- que le da respuesta

Compilador: Un compilador es un programa informático que traduce un programa escrito en un lenguaje de programación a otro lenguaje de programación, generando un programa equivalente que la máquina será capaz de interpretar.

CPU: La unidad central de procesamiento, o CPU (por el acrónimo en inglés Central Processing Unit), o simplemente, el procesador, es el componente en una computadora digital que interpreta las instrucciones y procesa los datos contenidos en los programas de la computadora.

Cracker: Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de éste último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

Criptografía: La criptografía es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Defacer: Es un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etcétera.

DSP: DSP es el acrónimo de Digital Signal Processor que significa Procesador Digital de Señal. Un DSP es un sistema basado en un procesador o microprocesador que posee un juego de instrucciones, un hardware y un software optimizados para aplicaciones que requieran operaciones numéricas a muy alta velocidad.

Función hash: Las funciones de hash de una vía (one-way) son una construcción criptográfica empleada en muchas aplicaciones. Son usadas junto con los algoritmos de clave pública para cifrado y firma digital.

Hackeo: Se suele llamar hackeo y hackear a las obras propias de un hacker; obtener información sin modificarla.

Hardware: Hardware corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente al soporte lógico e intangible que es llamado software.

Host: Máquina conectada a una red la cual tiene un nombre que la identifica, el hostname. La máquina puede ser una computadora, un dispositivo de almacenamiento por red, una impresora, etcétera.

IDS: Un sistema de detección de intrusos (o IDS por sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a una computadora o a una red. Estos accesos pueden ser ataques de habilidosos hackers o de script kiddies que usan herramientas automáticas.

Linux: GNU/Linux es el término empleado para referirse al sistema operativo Unix-like que utiliza como base las herramientas de sistema de GNU y el núcleo Linux. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL de GNU (Licencia Pública General de GNU) y otras licencias libres.

Malware: Malware (del inglés malicious software, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su

dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware.

Modelo cliente/servidor: Arquitectura distribuida que permite a los usuarios finales obtener acceso a la información en forma transparente aun en entornos multiplataforma. En el modelo cliente servidor, el cliente envía un mensaje solicitando un determinado servicio a un servidor (hace una petición), y éste envía uno o varios mensajes con la respuesta (provee el servicio)

Módem: Un módem es un dispositivo que sirve para modular y desmodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora

Proceso de Cifrado: El cifrado es el proceso de convertir el texto plano en un galimatías ilegible, denominado texto cifrado o criptograma.

TCP: TCP (Transmission-Control-Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet.

Red de comunicaciones: Conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etcétera) y servicios (acceso a internet, e-mail, chat, juegos).

Resetear: Término utilizado para describir el proceso de extraer una tarjeta de expansión o una RAM de la placa madre de la computadora y luego ponerla nuevamente en el mismo zócalo o slot del cual fue extraído.

Resets: Es la puesta en condiciones iniciales de un sistema. Éste puede ser mecánico, electrónico o de otro tipo. Normalmente se realiza al conectar el mismo, aunque habitualmente, existe un mecanismo, normalmente un pulsador, que sirve para realzar la puesta en condiciones iniciales manualmente.

Script Kiddie o Script Boy: Un Script Kiddie es un cracker inexperto que usa programas, scripts, exploits, troyanos, nukes, etcétera, creados por terceros para romper la seguridad de un sistema. Suele presumir de ser un hacker o cracker cuando en realidad no posee un grado relevante de conocimientos.

Seguridad: La seguridad consiste en mantener libre de peligro, daño o riesgo un activo (informático o no).

Software: La palabra software se refiere al equipamiento lógico o soporte lógico de una computadora digital, y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

Spyware: Un programa espía, traducción del inglés spyware, es un software, dentro de la categoría malware, que se instala furtivamente en una computadora para recopilar información sobre las actividades realizadas en ella. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

Texto Cifrado: Texto cifrado es aquel texto que ha sido transformado con algún algoritmo determinado y clave de cifrado.

Texto en Claro: Los archivos de texto plano (en inglés plain text) son aquellos que están compuestos únicamente por texto sin formato, sólo caracteres. Estos caracteres se pueden codificar de distintos modos dependiendo de la lengua usada.

UDP: UDP (User Datagram Protocol (en español Protocolo de Datagrama de Usuario) es un protocolo del nivel de transporte basado en el intercambio de datagramas.

Viruxer: Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

APÉNDICE B

Sensores Biométricos

APÉNDICE B SENSORES BIOMÉTRICOS

SENSOR DE HUELLAS DACTILARES

Existen dos técnicas para realizar la verificación de las huellas:

I. Basada en detalles: Esta técnica elabora un mapa con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza esta aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos. Entre algunos detalles que se pueden encontrar en una huella, se observan en la Figura B.1:

Figura B.1 Detalles en una huella dactilar.

Cada individuo posee sólo un arreglo de detalles (Figura B.2).

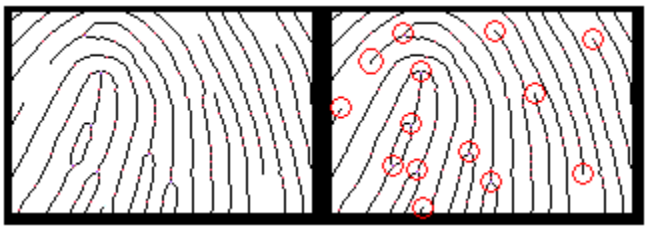


Figura B.2 Trazado del patrón de detalles

II. Basadas en correlación: Este método viene a mejorar algunas dificultades presentadas por la aproximación creada por el patrón de detalles, pero inclusive él mismo presenta sus propias fallas, esta técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen.

Una vez obtenida la huella digital es necesario clasificarla. Este proceso consiste en ubicar dicha huella dentro de los varios tipos existentes, los cuales proveen un mecanismo de indexado; esto con la finalidad de reducir el tiempo de búsqueda.

Los algoritmos existentes permiten clasificar la huella en 4 clases (Véanse figuras B.3, B.4, B.5, B.6):

- Lazo

Figura B.3 Clase lazo

- Arco

Figura B.4 Clase arco

- Espiral o circular

Figura B.5 Clase espiral

- Compuesta

Figura B.6 Clase compuesta

Estos algoritmos separan el número de crestas presentes en cuatro direcciones (0°, 45°, 90° y 135°) mediante un proceso de filtrado de la parte central de la huella.
Dentro del proceso de reconocimiento se emplean técnicas muy robustas que no se vean afectadas por algún ruido obtenido en la imagen además de que incrementan la precisión en tiempo real (Figura B.7).

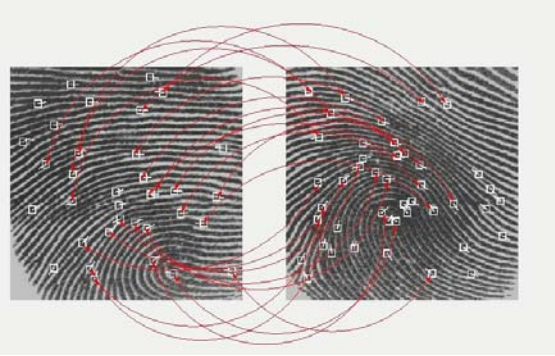


Figura B.7. Proceso de comparación.

Existen dos arreglos típicos de sensores de huellas dactilares:

I. Sensor de matriz capacitivo: La ventaja de este sensor es su simplicidad.

   Para dedos jóvenes, saludables y limpios, este sistema trabaja adecuadamente. Los problemas comienzan a presentarse cuando se tienen condiciones menos óptimas en la piel.

   Cuando el dedo está sucio, con frecuencia no existirán aberturas de aire en los surcos de la huella. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento.

II. Sensor de matriz de antena: Estos dispositivos no dependen de las características de la superficie, tales como las aberturas de aire entre el sensor y el surco.

En la figura B.8 se puede observar la forma típica de un sensor de reconocimiento de huellas dactilares.

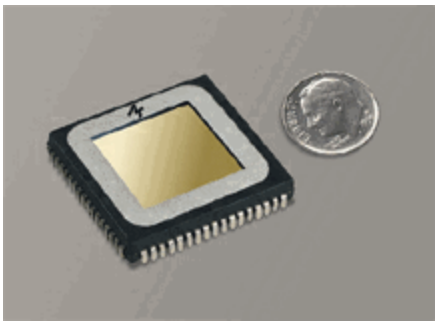


Figura B.8 Sensor de huellas dactilares

RECONOCIMIENTO DEL IRIS

Patrón del iris

El propósito del reconocimiento del iris es obtener en tiempo real, con alto grado de seguridad, la identidad de una persona; empleando análisis matemático del patrón aleatorio que es visible dentro del ojo a cierta distancia.

En sistemas para el reconocimiento del iris es común encontrar cámaras de video de tipo CCD (Dispositivo de Carga Acoplada). Este dispositivo consiste de varios cientos de miles de elementos individuales (pixeles) localizados en la superficie de un circuito integrado.

Cada pixel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la cámara), almacenando una pequeña carga de electricidad. Los pixeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales).

En la figura B.9 se puede apreciar un sensor de tipo CCD.

Figura B.9 Sensor CCD

APÉNDICE C

Jefatura y Secretaría

JEFATURA Y SECRETARÍA[23]

1. IDENTIFICACIÓN DE ACTIVOS

Se identifica que las actividades de jefatura y secretaría son muy similares, las cuales son el brindar atención a alumnos y profesores, trabajando en conjunto para la planeación, evaluación de actividades relacionadas con el apoyo académico.

En cuanto a la Secretaria Auxiliar, sus principales actividades son, realizar el trámite de la contratación del personal académico, de actas para extraordinarios, elaboración de nombramientos y corrección de calificaciones.

El papel de la Secretaría (Académica y Auxiliar) es ser el enlace entre la Jefatura de la división y los jefes de cada departamento, el personal académico y los alumnos.

Una vez definidas las actividades se realiza la identificación de los activos correspondientes, los cuales son:
Quitarlo de la tabla ponerlo como viñetas en los incisos correspondientes, a) Jefatura y Secretaría Académica, b) Secretaría Auxiliar

a) Jefatura y Secretaría Académica

- Computadoras.
- Impresoras.
- Escáner.
- Quemador externo.
- Fotocopiadora.
- Máquina de escribir.
- Equipo de proyección.
- Bases de datos.

b) Secretaría Auxiliar

- Bases de datos.
- Acceso a sistemas externos.
- Archiveros.

2. IDENTIFICACIÓN DE AMENAZAS

Las amenazas identificadas son las siguientes:

- Falla en los equipos o dispositivos que almacenan o manipulan la información.

[23] Ver cuestionarios en el apéndice D

- Problemas con los equipos conectados a la red.
- Lentitud en la respuesta cuando se trabaja con la red.
- Problemas con el acceso a Internet.
- Se presentan infecciones en los equipos de cómputo (gusanos, virus, programas maliciosos, etcétera).
- No dar aviso de cortes de los servicios de red.
- Revelación de la información confidencial por el personal que la manipula.

3. IDENTIFICACIÓN DE VULNERABILIDADES

Las vulnerabilidades identificadas son las siguientes:

- No contar con no-breaks suficientes para los equipos de cómputo.
- No se tiene control de acceso a la información contenida en los archiveros (no se cuenta con chapas en los archiveros).
- Al instalar un equipo nuevo, sólo en algunos casos se da lectura a los manuales adjuntos, lo que provoca la presencia de vulnerabilidades de tipo de hardware.
- No se cuenta con métodos de control de acceso para la entrada al edificio.
- No contar en algunos casos con políticas de seguridad del departamento, o al menos no conocidas por los empleados.
- No conocer las políticas de seguridad de la institución.
- En general la administración de la red se considera adecuada a excepción de la decisión de la denegación de servicios sin aviso previo.
- No se verifican los perfiles del personal a ser contratado o del personal que envía la Dirección de Personal.
- El personal no cuenta con conocimientos sobre algún plan de contingencia ante un sismo o desastre que ponga en peligro los activos. Ya que al parecer no se cuenta con un plan de contingencia.

4. IMPACTO DE LA OCURRENCIA DE UNA AMENAZA

A continuación se mencionan posibles impactos con base en las vulnerabilidades y amenazas descritas anteriormente.

- La falla de equipos o dispositivos de almacenamiento, así como el equipo conectado~~s~~ a la red, o la denegación de servicios de red**,** sería un ataque hacia el servicio de disponibilidad de la información.

- La presencia de virus o códigos maliciosos en los equipos de cómputo ocasionaría un ataque hacia el servicio de la Integridad de la información.

- El no contar con no-breaks en los equipos, ocasionaría daños en los mismos que se reflejaría como pérdidas económicas para la institución, además de ser un ataque al servicio de disponibilidad de la información.

5. CONTROLES EXISTENTES

Dentro de los controles identificados se resume lo siguiente:

I. Controles Requeridos:

- En la Jefatura, se implementan medidas recomendadas por la COMISIÓN LOCAL DE SEGURIDAD.

- En el caso de Secretaría Académica y Auxiliar, no se cuenta con algún reglamento para el control de activos.

II. Controles Discrecionales:

- Uso de algún antivirus.

- Respaldo de la información.

- Control en el resguardo del equipo.

- En el caso de la Secretaría Auxiliar, mantener siempre la puerta de la oficina cerrada, además de la implementación de una conexión punto a punto (dos computadoras), donde el uso está restringido por las personas que ahí laboran.

6. RIESGOS RESIDUALES

Áreas que conforman el Departamento de Jefatura y Secretaría Académica:

- Jefatura

- Secretaría Académica
- Sala de Juntas
- Zona Secretarial
- Área de Técnicos Académicos
- Área de Fotocopiado

De las áreas anteriormente citadas se tiene alta vulnerabilidad en las áreas de Secretaría Académica y Jefatura.

Para reforzar la seguridad de los activos dentro del área se considera que es necesario controlar los accesos, contar con personal de vigilancia (competente), ya que el riesgo de pérdida de equipo es latente.

7. CONTROLES ADICIONALES

Con base en el análisis realizado anteriormente algunas recomendaciones para disminuir las vulnerabilidades citadas son:

- Contar con no-breaks para el cuidado de los dispositivos y de los equipos de cómputo.
- Implementar controles de acceso tanto en la entrada del edificio como en cada uno de los departamentos.
- Contar con cuentas de usuario para cada persona que usa los equipos de cómputo.
- Difundir en el personal las Políticas de Seguridad implementadas en la institución.
- Contar con políticas particulares para el área y difundirlas entre las personas que ahí laboran.
- Se notifique con anticipación cualquier decisión tomada por los administradores, como por ejemplo la denegación de puertos y servicios.
- Tomando en cuenta la observación de que no se tiene un plan de contingencia o se desconoce, crear uno y difundirlo.
- Llevar el control por medio de una bitácora para conocer las causas por las cuales ha fallado el equipo o se han suscitado problemas.
- Realizar un mantenimiento periódico de los equipos de cómputo para tener un funcionamiento óptimo y con ello se permitan realizar las actividades correspondientes.

APÉNDICE D

Cuestionarios

1. DEPARTAMENTO DE COMPUTACIÓN

1. ¿Qué tipo de información se maneja en su lugar de trabajo?
2. Enliste de mayor a menor los activos o bienes que considere más importantes en su área de trabajo
3. ¿Cuenta con algún inventario sobre el equipo en uso y desuso que se encuentra en su cubículo?
4. ¿Qué tipo de problemas se han presentado últimamente?
5. En caso de haber existido problemas, ¿qué medidas se han tomado con respecto a éstos?
6. En su opinión, ¿cuáles son los puntos débiles que se presentan en su lugar de trabajo?
7. ¿Qué tipo de aplicaciones o programas utiliza?
8. ¿Utiliza programas para descargar archivos de internet? ¿Cuáles utiliza?
9. ¿Utiliza programas de mensajería instantánea?
10. Si se denegaran los puertos o algún otro servicio, ¿cómo afectaría esto en sus actividades?
11. Si esto ha sucedido, ¿a usted le han avisado sobre esta medida?
12. ¿Cómo califica el aviso sobre esta medida y cómo le gustaría que fuera si se volviera a presentar?
13. ¿Se cuenta con control de acceso a los cubículos?
14. ¿Se tienen implementadas medidas de seguridad en el cubículo para el resguardo de la información?
15. ¿Está de acuerdo con la aplicación de un análisis de riesgo?
16. Si su respuesta es afirmativa, ¿usted fue avisado sobre el análisis?
17. ¿Considera que fue avisado oportunamente sobre dicho análisis?
18. ¿Cómo califica el nivel de seguridad de su área de trabajo?

Elija: Excelente Bueno Regular Malo Pésimo

LABORATORIOS

1. ¿Qué tipo de información se maneja en el laboratorio?
2. Enliste de mayor a menor los activos o bienes que considere más importantes en el laboratorio
3. Si se denegaran los puertos o algún otro servicio, ¿cómo afectaría esto en sus actividades?
4. ¿Cuenta con algún sistema de verificación de los sistemas, así como de los empleados?
5. ¿Cuenta con contraseñas robustas?
6. ¿Cuenta con un registro para el control de acceso al laboratorio?
7. ¿Cuenta con los estados actuales de los parches de seguridad?
8. ¿Cómo se gestionan las copias de seguridad y su almacenamiento externo?
9. ¿La información que se maneja en el servidor se encuentra cifrada?
10. ¿Los algoritmos criptográficos y las herramientas asociadas son válidas?
11. ¿Han sido eliminados todos los procesos innecesarios de los equipos?
12. ¿Conoce la diferencia entre ataques internos o ataques externos?
13. ¿Conoce la norma ISO 27001?
14. ¿Conoce las políticas de seguridad del departamento y de la facultad?
15. ¿Cuenta con la divulgación de políticas de seguridad y procedimientos establecidos?

16. ¿Cuenta con un análisis de riesgos para dar una mayor seguridad a la organización?
17. ¿Con qué mecanismos de seguridad cuenta el departamento o laboratorio?
18. ¿Cómo son difundidas las medidas de seguridad dentro del departamento o laboratorio?
19. ¿Tienen los encargados del laboratorio autorización necesaria para el acceso a archivos o programas?
20. ¿Cuenta con planes de contingencia dentro del departamento?
21. ¿Cuenta el laboratorio o departamento con el mantenimiento necesario para las aplicaciones tanto en software como en hardware?
22. ¿Cuenta el personal autorizado con los suficientes privilegios para acceder a la información como por ejemplo bases de datos, etcétera?
23. ¿Cuenta el laboratorio con el uso de antivirus y firewalls para resguardar la seguridad de la información?
24. ¿Con qué frecuencia se actualizan los antivirus y firewalls?
25. ¿Cuenta el departamento o laboratorio con soporte técnico en caso de alguna falla que pudiera dañar los sistemas y equipos o la seguridad?
26. Al final de cada turno, ¿Se controla el número de entradas y salidas del personal?
27. ¿Cree Ud. que los Controles de acceso son adecuados?
28. ¿Cuenta con algún inventario sobre el equipo en uso y desuso que se encuentra en el laboratorio?
29. ¿Qué tipo de problemas se han presentado últimamente en el laboratorio?
30. En caso de haber existido problemas, ¿qué medidas se han tomado con respecto a éstos?
31. En su opinión, ¿cuáles son los puntos débiles que tiene el laboratorio?
32. ¿El laboratorio cuenta con servicio abierto para el alumnado?, si es así, ¿cuáles son las medidas en cuanto al control de acceso con las que cuenta el laboratorio?
33. ¿Está de acuerdo con la aplicación de un análisis de riesgo?
34. Si su respuesta es afirmativa, ¿usted fue avisado sobre el análisis?
35. ¿Considera que fue avisado oportunamente sobre dicho análisis?
36. ¿Cómo califica el nivel de seguridad de su área de trabajo?
    Elija: Excelente Bueno Regular Malo Pésimo

2. DEPARTAMENTO DE CONTROL

1. ¿Cuántas personas laboran en este departamento?
2. ¿Con cuántos equipos de cómputo cuentan?
3. ¿Cuántas cuentas por usuarios se tienen?
4. ¿Qué tipo de información manejan?

5. ¿Qué tipo de información considera de mayor importancia?
6. ¿Quién tiene acceso a esa información?
7. ¿Qué hace o haría para resguardar esa información?
8. ¿Sabe qué es un firewall?
9. ¿Sabe si los equipos cuentan con un firewall?
10. ¿Sabe que es un antivirus?
11. ¿Qué antivirus conoce?

12. ¿Sabe si los equipos cuentan con un antivirus, cuál?
13. ¿Las cuentas de usuarios de equipos tienen contraseña?
14. ¿Conoce las recomendaciones para elegir una buena contraseña?
15. ¿Sabe si las contraseñas se cambian periódicamente?
16. ¿Sabe qué es un puerto de comunicación?
17. ¿Qué actividades importantes se realizan en el departamento?
18. ¿Cuáles serían las consecuencias si existiera pérdida de información?
19. ¿Sabe a qué se refiere el término activo?
20. ¿Cuáles serían los activos con los que cuenta?
21. ¿Cuáles serían las consecuencias si existieran pérdidas de activos?
22. ¿Sabe qué es una amenaza?
23. ¿Qué tipo de amenazas conoce?

Amenaza	
Humanas	
Errores de hardware	
Errores en la red	
Problemas de tipo lógico	
Naturales	

24. ¿Con qué frecuencia se presentan estas amenazas?
25. ¿Sabe qué es una vulnerabilidad?
26. ¿Qué tipo de vulnerabilidades conoce?

Vulnerabilidad	
Física	
Natural	
De software	
De hardware	
De red	
Humanas	

27. ¿Qué tipo de vulnerabilidades se presentan con mayor frecuencia?
28. ¿Sabe qué es un ataque?
29. ¿Cuando se presenta un ataque, se imagina cuál ha sido el objetivo del atacante?
30. ¿Cuáles han sido las consecuencias de dicho ataque?
31. ¿Sabe qué es una medida de seguridad?
32. ¿Qué medidas de seguridad conoce?
33. ¿Con qué medidas de seguridad se cuenta~~n~~ con el departamento?
34. Tomando en cuenta las medidas existentes y los ataques sufridos ¿Qué otras medidas implementaría?

3. DEPARTAMENTO ELÉCTRICA DE POTENCIA

Seleccione la respuesta correcta:

1. ¿Qué puede hacer un virus informático?

a) Cambiar el modo en que funciona el equipo.

b) Cambiar el modo en que funciona el sistema.
c) Provocar que el equipo se bloquee y se tenga que reiniciar cada cierto tiempo.
d) Cualquiera de las anteriores.

2. Al recibir un archivo adjunto inesperado en un mensaje de correo electrónico de un conocido debe:

a) Abrir el archivo adjunto y guardarlo en el disco.
b) Abrir el archivo adjunto, pero si tiene virus cerrarlo inmediatamente.
c) Enviar un mensaje de correo electrónico al remitente para comprobar que realmente quería enviarlo antes de abrir el archivo adjunto.
d) Responder al correo electrónico y preguntar por el contenido del archivo adjunto.

3. Si un virus ha infectado el equipo, ¿cuál de las siguientes herramientas pueden ayudarle a suprimirlo? (Elija la mejor respuesta.)

a) Un servidor de seguridad de Internet y software antivirus.
b) La herramienta de eliminación de software malintencionado de Microsoft y software antivirus.
c) La herramienta de adición de software benigno de Microsoft y Windows AntiSpyware (Beta).
d) Actualizaciones automáticas de Microsoft Windows y las herramientas de usuario.

4. La mensajería instantánea es una forma estupenda de charlar con los amigos en línea sin preocuparse de los virus.

a) Verdadero
b) Falso

5. ¿Qué puede dañar un virus?

a) Conectividad a Internet
b) Software
c) Hardware
d) Todas las anteriores

6. Después de instalar un software antivirus en el equipo, no hay que preocuparse por un ataque de virus en él.

a) Verdadero
b) Falso

7. Acabo de comprar software nuevo y el programa de instalación me indica que desactive mi software antivirus. ¿Cuál es la mejor forma de afrontar esta situación y que el equipo siga protegido?

a) Desactive el software antivirus durante la instalación y, a continuación, vuelva a activarlo cuando haya terminado.
b) Es un mensaje de error habitual. Omítalo y continúe con la instalación.
c) El programa antivirus es incompatible con el nuevo software; tendrá que quitarlo por completo.
d) Detenga la instalación y vuelva a intentarlo, pero no desactive el software antivirus.

8. Las cuentas de usuario en su equipo pueden protegerle de los virus porque:

a) Proporcionan un sistema de pago en línea seguro.
b) Determinan quién puede instalar o quitar software.
c) Controlan las contraseñas.

d) Determinan lo que se muestra al enviar un mensaje de correo electrónico.

9. Recibe un mensaje instantáneo de alguien que conoce que tiene adjunta una imagen divertida de un pollito. ¿Cuál es la forma más prudente de tratar este tipo de archivos adjuntos?

a) Parece que procede de un amigo, pero puede descargar un virus en el equipo.
b) Es de un amigo y puede hacer algo divertido.
c) Es de un amigo, pero debo responderle para preguntarle si realmente lo ha enviado.
d) ¿Qué daños puede causar un pollito?

10. No supone ningún riesgo especial introducir datos personales o financieros en una ventana emergente.

a) Verdadero
b) Falso

11. ¿Cómo se sabe si un sitio Web ofrece seguridad para ayudarle a proteger datos importantes?

a) Aparece un pequeño icono amarillo en forma de candado en la parte inferior de la ventana del explorador.
b) Sus amigos compran siempre en ese sitio Web y nunca han tenido ningún problema.
c) Ha descubierto el sitio Web a través de un motor de búsqueda en línea.
d) El certificado de seguridad del sitio coincide con el nombre del sitio.

12. ¿Qué debería hacer si cree que ha sufrido una estafa de "phishing"?

a) Informar a la empresa cuya dirección de correo electrónico o cuyo sitio Web se ha falsificado.
b) Cambiar las contraseñas de todas sus cuentas.
c) Comprobar los extractos bancarios de inmediato.
d) Todas las anteriores.

13. Verdadero o falso: El software antivirus puede ayudarle a protegerse de las estafas de "phishing".

a) Verdadero
b) Falso

14. De los siguientes síntomas, ¿cuál NO suele ser indicio de que un mensaje de correo electrónico es fraudulento?

a) Se le pide que haga clic en un vínculo del mensaje para facilitar datos acerca de su cuenta.
b) Parece urgente.
c) Se dirige a usted por su nombre y apellido(s).
d) Se le pide que confirme datos personales.

15. ¿Cómo se puede saber si un mensaje de correo electrónico relacionado con la seguridad que parece proceder de Microsoft es auténtico?

a) Se le piden los datos de la tarjeta de crédito para validar su copia de Microsoft Windows.
b) El mensaje contiene un archivo adjunto.
c) Al hacer doble clic en el icono del candado que se encuentra en la barra de estado se muestra un certificado de seguridad emitido para el mismo nombre de dominio (www.microsoft.com) que el que figura en la barra de direcciones.

4. DEPARTAMENTO DE ELÉCTRONICA

1. ¿Cuál es la principal actividad que desempeña?
2. Para el desempeño de sus actividades, ¿Qué considera que es lo más importante?
3. Acerca del equipo de cómputo ¿Qué utilidad le da?
4. La información que tiene en su equipo de cómputo ¿Esta respaldada? En caso afirmativo ¿Qué medio utiliza para su respaldo?
5. ¿Cuenta con alguna medida de seguridad para la protección de su equipo electrónico?
6. ¿Su equipo cuenta con contraseña? Si es así ¿Ésta le fue dada por el administrador de la red?
7. ¿Cuenta con acceso a red?
8. ¿Cuál sería el uso más importante para lo que utiliza la red?
9. ¿Cuenta con algún antivirus? En caso de contar con él. ¿Cuál es?
10. ¿Su máquina se ha infectado por algún tipo de virus?
11. ¿De qué forma obtiene el software que necesita? ¿Tiene algún conocimiento sobre el control de instalación de programas?
12. ¿Qué personas tienen acceso a su área de trabajo?
13. ¿Ha tenido alguna experiencia de extravío o robo de algún bien dentro del cubículo?
14. ¿Tiene conocimiento de alguna política de seguridad o plan te continencia establecidas por el departamento?

5. DEPARTAMENTO DE PROCESAMIENTO DE SEÑALES

1. Podría describir las principales actividades que este laboratorio lleva a cabo
2. De estas actividades cuáles son las que presentan inconvenientes en su realización (de manera más frecuente)
3. El personal que labora en este departamento, ¿conoce las políticas de seguridad informática de la institución?
4. Podría mencionar qué políticas de seguridad informática conoce usted
5. Con qué bienes cuentan en este departamento (bienes materiales; información única y relevante)
6. Dentro de los bienes con los que cuenta este laboratorio cuáles considera que tienen un mayor valor (cuáles son más importantes, imprescindibles)
7. ¿Cuáles serían las características más relevantes de cada uno de estos bienes?, ¿Cómo se implementan y se utilizan?
8. Aproximadamente cuál es el valor monetario de estos bienes
9. ¿Cual es la jerarquía de los activos (bienes), esto es, dependen unos de otros?
10. El personal que opera estos activos, ¿tiene la capacitación necesaria para utilizarlos adecuadamente?, ¿existe capacitación continua para dicho personal?
11. Se realizan evaluaciones al personal para determinar su nivel de conocimientos antes de ser elegidos para desarrollar cierta actividad dentro del departamento.

12. ¿Qué consecuencias traería al laboratorio la pérdida o falla de alguno de los activos?
13. ¿Cuáles serían las acciones a tomar para resolver las situaciones no previstas que se presenten, de manera rápida, o para poder seguir operando con la mayor normalidad posible en ese momento?
14. ¿Cuáles serían los puntos débiles (vulnerabilidades) de sus activos?
15. El laboratorio ha sufrido algún tipo de amenaza, o ha atravesado por algún problema mayor que haya causado pérdida de información o recursos materiales, a causa de personas externas, mal manejo del personal o desastres naturales
16. ¿Los activos están protegidos de manera adecuada y segura, cuentan con algún tipo de seguro?
17. ¿Cuenta con algún tipo de seguridad en este departamento? ¿Cuál?
18. ¿Con qué medidas de seguridad cuentan?
19. ¿Cómo son implementadas estas medidas?
20. ¿Quién es el responsable de verificar que éstas se lleven a cabo?
21. Son suficientes estas medidas de seguridad para evitar contratiempos en el desarrollo de las actividades normales del departamento
22. Si no cuentan con medidas de seguridad, ¿consideraría importante implementar una serie de éstas para poder operar de manera correcta y prevenir así situaciones difíciles?
23. ¿Qué medidas de seguridad cree usted que serían necesarias para mejorar las actividades del departamento?
24. Si usted se encuentra laborando como regularmente lo hace y en cierto momento su máquina comienza a realizar los procesos de forma más lenta o extraña, ¿qué haría para resolver esto?
25. Si nota que alguien ha entrado a su sesión sin su permiso y que además su información ha sido modificada, ¿qué serie de problemas se generarían?
26. ¿Cómo resolvería esta situación?, ¿existen medidas precautorias para evitar esta situación?
27. Si existen sesiones para cada uno de los elementos del personal que labora en el departamento ¿se les ha hecho saber que por ningún motivo deben compartir contraseñas? ¿se ha suscitado algún percance de esta naturaleza?
28. Alguna persona ajena a las instalaciones del laboratorio intenta ingresar a alguna de las áreas sin autorización, ¿existe alguna medida para evitar esto?
29. Si la persona extraña intenta modificar la información, intenta o roba algo se notaría de inmediato, o podría pasar desapercibido. ¿Qué se haría en tal situación?
30. ¿Cuántas personas laboran en este laboratorio, y cómo se controla su acceso al mismo?
31. ¿El personal del laboratorio tiene acceso a todos los bienes del mismo sin restricción?, ¿Existe un control en el manejo de bienes e información?, menciónelo
32. Dentro de su personal ¿hay algún elemento que sea indispensable para el funcionamiento de gran porcentaje de las actividades realizadas en el laboratorio? En caso afirmativo ¿qué medidas se tomarían si este elemento no pudiera estar al frente de sus tareas?

33. ¿Enfrenta problemas para poder desarrollar sus actividades de manera normal, de forma frecuente o casi nunca?

6. DEPARTAMENTO DE SISTEMAS ENERGÉTICOS

1. ¿Qué puesto tiene?
2. ¿Qué carrera tiene?
3. ¿Qué conocimientos tiene en Computación?
4. ¿Qué trabajo realiza en el departamento de Sistemas Energéticos?
5. ¿Cuáles son los nombres del personal responsable del departamento donde laboran?
6. ¿Cuál es su horario de trabajo?
7. ¿En dónde está ubicado?
8. ¿Cuántos laboratorios tiene?

a)1 b)2 a 4 c) más de 4 d) No sé.

9. ¿Cuántos cubículos tiene?
10. ¿Qué tipo de información maneja?
11. ¿Qué ocurre si no hay disponibilidad de la información de Internet?
12. ¿Cuenta con información impresa del(os) trabajo(s) que realiza(n)?

a) Sí b) No c) No lo recuerdo.

13. ¿Hace respaldos de la información que realiza en su trabajo?

a) Sí b) No c) No lo recuerdo.

14. ¿Actualiza los respaldos de la información que hace?

a) Sí b) No c) No lo recuerdo.

15. ¿Hay respaldos de la información que utiliza diariamente?

a) Sí b) No c) No lo recuerdo.

16. ¿Qué haría si se perdieran sus respaldos?
17. ¿Qué sucedería si alguien no autorizado tiene acceso su información?
    a) Se sanciona a la persona responsable del acceso de la información.
    b) Nada
    c) Se prohibirían las visitas al departamento sin previa cita.
18. ¿Se cuenta con servicio de impresión?

a) Sí b) No ¿Por qué no?

19. ¿Cómo protege su información y respaldos (de pérdidas, robos, etcétera)?
    a) En un cajón con llave
    b) No diciéndole a nadie
    c) Otra(s) ¿Cuál(es)?
20. ¿Ha perdido información a causa de un ataque?

a) Sí b) No c) No lo recuerdo.

21. ¿Qué es lo más valioso que tiene para realizar su trabajo?

a) Su computadora b) Su memoria USB c) Otro(s) ¿Cuál(es)

22. ¿Qué paqueterías usa?

a) Office
b) Adobe creator
c) Matlab
d) Messenger
e) Otro(s) ¿Cuál (es)?

23. ¿Hay copias de seguridad de los programas?
a) Sí ¿Cuáles?
b) No
c) No lo recuerdo.
d) No sé
24. ¿Cuántos equipos tienen y cuáles son sus características?
25. ¿Está conectado a alguna red local?
a) Sí b) No c) No sé
26. ¿Tiene acceso a Internet?
a) Sí b) No
27. ¿Qué ocurre si no hay disponibilidad de Internet?
a) No realiza su trabajo
b) Busca dónde puede conectarse a Internet
c) No sé
28. ¿Alguna vez se ha quedado sin servicio de Internet?
a) Sí
b) No
c) No lo recuerdo.
29. En el caso de que haya sucedido lo de la pregunta anterior, ¿hace cuánto que sucedió?
30. ¿Se le avisa al usuario que no habría servicio de Internet?
a) Sí b) No ¿Por qué no lo hicieron? c) No sé
31. ¿Cuenta con instrumentos de medición?
    a) Sí ¿cuáles?
    b) No
32. ¿Hay una persona encargada de encender las computadoras?
    a) Sí ¿Quién (es)?
    b) No
    c) Otro(s) ¿Cuál (es)?
33. ¿Qué tiempo están encendidas las computadoras?
    a) 1 hora
    b) 2 a 3 horas
    c) más de 3 horas
    d) No sé
34. ¿Con qué frecuencia se hace un escaneo a las computadoras para verificar si hay un virus u otra cosa?
    a) Cada mes b) Cada seis meses c) Cada año c) Más de un año
35. ¿Han sufrido fallas en las computadoras?
    a) Sí. ¿Qué fallas han sucedido?
    b) No
36. ¿Qué es lo que se hace cuando se presenta alguna falla en su computadora?
    a) La reviso yo mismo.
    b) No hago nada.
    c) No sé.
    d) Otro(s) ¿Cuáles?
37. ¿Con qué frecuencia hay fallas en su computadora?
    a) Cada mes
    b) Cada 6 meses

c) Cada año
d) Otro ¿Cuál?

38. ¿Tiene comunicación con otros lugares del Departamento de Sistemas Energéticos?
    a) Sí
    b) No
39. ¿Existen planes de mejora al área de trabajo?

a) Sí b) No c)No sé

40. ¿Cuenta con políticas de seguridad en el área de trabajo?
    a) Sí
    b) No ¿Por qué?
41. Si la respuesta anterior es sí entonces ¿están a la vista de todos los usuarios?
    a) Sí
    b) No
42. ¿Cuenta con un plan de contingencias?
    a) Sí
    b) No ¿Por qué?
43. ¿Qué hace si algún equipo se pierde?
    a) Se busca el equipo
    b) Se reemplaza el equipo por otro
    c) Se compra otro equipo
    d) Otro ¿Cuál?
44. ¿Se puede remplazar algún equipo?

a) Sí b) No

45. Si la respuesta anterior es sí ¿cuánto tiempo tardaría en reemplazarse?

a) Una semana b) Un mes c) Más de un mes d) No lo sé.

46. ¿Cuál es el valor económico de cada equipo?
47. ¿Se va la luz?

a) Sí b) No c) No sé.

48. Si su respuesta anterior es sí entonces ¿qué hace si se va la luz?

a) No trabaja b) Hacer otra cosa c) Otra ¿Cuál?

49. Si la respuesta de la pregunta 47 es no, entonces ¿qué pasaría si se va la luz?
    a) Se reporta la falla de energía eléctrica
    b) No sé
    c) Otra ¿Cuál?
50. ¿Tiene un no break?

a) Sí b) No

51. ¿Qué se necesita para poder tener acceso a las computadoras del laboratorio?
    a) Anotarse en una libreta
    b) Estar dado de alta en la base de datos
    c) Mostrar credencial de la escuela o que trabaja en el departamento
    d) Nada
    e) Otro ¿cuál?
52. En caso de no contar con lo que se requiere en la pregunta anterior entonces ¿Se requiere de otro requisito?

a) Sí ¿Cuál? b) No

53. Si se presenta una falla, ¿sobre quién recae la responsabilidad?

54. ¿Quién(es) se queda(n) cuidando el área de trabajo mientras es la hora de comida?
    a) La secretaria
    b) El encargado del departamento
    c) Otro ¿Quién?
55. ¿Cuántas personas tienen acceso al laboratorio por día?

a) 5 personas b) 6 a 15 personas c) más de 15 personas

56. ¿Falla mucho la conexión de Internet?
    a) Sí ¿Por qué?
    b) No
57. ¿Cuántos usuarios utilizan la sala de cómputo?
58. De los usuarios que utilizan las máquinas, ¿todos están registrados en su sistema?
59. ¿Qué se necesita para darse de alta en su sistema?
    a) Credencial
    b) Trabajar en el departamento.
    c) Tener un proyecto.
    d) Otro(s). ¿Cuál (es)?

60. ¿Puede entrar un usuario que no sea del Departamento de Sistemas Energéticos?
    a) Sí
    b) No. ¿Qué medidas toman?
61. ¿Ha tenido problemas con la configuración del sistema en la red?

a) Sí b) No

62. Cuando se hace la limpieza, ¿alguien está presente?

a) Sí b) No

63. ¿Se cuenta con extinguidores en el área de trabajo en caso de un incendio?

a) Sí b) No

64. ¿Cuentan los equipos con mecanismos de seguridad?
    a) Sí ¿Cuáles?
    b) No
65. ¿Cuentan con ventilación o aire acondicionado los equipos de cómputo?

a) Sí b) No

66. ¿Cada cuánto tiempo se le da mantenimiento a todos los centros de cómputo de su dependencia?

a) Cada 6 meses b) Cada año c) Cada dos años d) Cada 3 años

67. ¿Todos los equipos de cómputo cuentan con licencias de los sistemas operativos y del software?

a) Sí b) No

68. ¿Permiten descargar software, videos, música o instalar algún programa?
    a) a) Sí b) No
69. ¿Qué controles de seguridad usa?

a) Cámaras de seguridad
b) Registro del personal en cada departamento
c) Libro de visitas

d) Otro(s) ¿Cuál(es)?

70. Para la administración de la red, ¿el sistema operativo está actualizado y debidamente configurado?

a) Sí b) No

71. ¿Cuántos servidores tiene?

a) Ninguno b) 1 c) 2 a 4 d) más de 4

72. Si su respuesta anterior es al menos uno o más de un servidor entonces diga ¿dónde se encuentran?
73. ¿Tiene inventarios de los equipos y dispositivos externos?
    a) Sí b)No
74. Diga ¿qué estándares utiliza para las redes de datos?
75. ¿Se tiene la lista de todo el personal que labora en el Departamento de Sistemas Energéticos?
    a) Sí. ¿Quién se hace cargo de la lista?
    b) No

76. ¿Hay alguna persona encargada de recoger los respaldos de la información más importante para el departamento en caso de un sismo, incendio, inundación, etcétera?
    a) Sí. Escriba el nombre.
    b) No hay.
77. ¿Se tiene botiquín de primeros auxilios? a) Sí b)No
78. ¿Se tienen redes inalámbricas? a) Sí b) No

Si es sí conteste las siguientes preguntas.

79. ¿Maneja cifrado? a) Sí b) No
80. ¿Maneja filtrado por MAC? a) Sí b) No
81. ¿Qué tipo de autenticación utiliza?

a) WEP b) WAP c) Otro(s) ¿Cuál(es)?

82. ¿Cuenta con punto de acceso?
    a) Sí ¿Cuántos tiene? b) No
83. ¿Cuántos equipos se conectan a la red?
    a) a) 5 equipos b) 6 a 15 equipos c) Más de 15 equipos
84. Si los servicios se niegan ¿qué hacen?
85. Si los servicios se niegan ¿se les avisa? a) Sí b) No
86. ¿Quién es el responsable de avisar que los servicios se están negando?
87. Si se niegan sin aviso ¿cuánto afecta sus actividades?

a) Mucho b) Poco c) Nada

7. DEPARTAMENTO DE TELECOMUNICACIONES

1. ¿Cuáles son los principales bienes que usted maneja? Entiéndase por bienes la información que utiliza, los equipos y todo aquello que sea importante dentro de su área de trabajo. Anótelos de acuerdo con su orden de importancia.
2. ¿Usted conoce los bienes con los cuales cuenta el departamento en el que labora? Anótelos de acuerdo con su orden de importancia.

3. ¿Qué sucedería si sus bienes se presiden? ¿Su recuperación sería costosa? ¿Qué tan costosa? Considere su costo en términos económicos, de tiempo y personales.
4. ¿Qué sucedería si los bienes del departamento se presiden? ¿Su recuperación sería costosa? ¿Qué tan costosa? Considere su costo en términos económicos, de tiempo y grupales.
5. ¿De qué manera protege sus bienes dentro del departamento? Refiérase a respaldos, extinguidores, cerraduras, contraseñas, y demás medidas de protección de bienes.
6. ¿Qué medidas de seguridad se utilizan en el cual labora para proteger los bienes del mismo?
7. Usted cuenta con medidas de protección para sus bienes dentro de su área de trabajo, en caso de ser así, éstas fueron establecidas por acuerdo del departamento o se rige por las establecidas en la institución, indique en qué caso se encuentra cada una.
8. ¿Qué ocurriría si la información confidencial con la que cuenta es conocida por otras personas? ¿Cuál sería el impacto si dicho acto ocurriera? Considere su costo en términos económicos, de tiempo y grupales.
9. ¿Qué ocurriría si la información con la que cuenta es modificada por otra persona de tal manera que los datos originales han sido alterados y no es posible restablecerlos? ¿Cuál sería el impacto si dicho acto ocurriera? Considere su costo en términos económicos, de tiempo y grupales.
10. ¿Qué ocurriría si la información con la que cuenta es eliminada, obteniendo así, una pérdida completa, de tal forma que los datos con los que se contaba no pueden ser recuperados bajo ninguna circunstancia? ¿Cuál sería el impacto si dicho acto ocurriera? Considere su costo en términos económicos, de tiempo y grupales.
11. ¿Qué tanto le afecta, cuando no existe temporalmente un servicio que para usted es indispensable usar en ese momento, por ejemplo: pérdida temporal del servicio de correo electrónico, en general, pérdida del servicio de Internet? ¿Cuál sería el impacto si dicho acto ocurriera? Considere su costo en términos económicos, de tiempo y grupales.
12. ¿Conoce reglas o medidas hechas por el administrador de la red o del departamento para que no se presenten los problemas mencionados anteriormente? En el caso de ser así, mencione cuáles son y enuméralas de acuerdo con el grado de importancia de manera ascendente, que usted le asigne.
13. Mencione usted qué programas de mensajería instantánea maneja:
    - ❖ Windows Live Messenger (MSN Messenger)
    - ❖ Yahoo! Messenger
    - ❖ AOL Messenger
    - ❖ Gmail Talk
    - ❖ Otro: _____
    - ❖ Ninguno.
14. Mencione si utiliza algún software de protección. Indique la versión que emplea:
    - ❖ Symantec Norton Antivirus
    - ❖ Symantec Norton Internet Security

- ❖ McAfee Antivirus
- ❖ McAfee Security Suite
- ❖ NOD32
- ❖ BitDefender
- ❖ Otro:_____
- ❖ Ninguno

15. ¿Utiliza programas para descargar información como videos, música, juegos, programas en general?
16. ¿Existen políticas en su departamento con respecto a los accesos que se tienen a las áreas con información sensible?
17. ¿De acuerdo con todo lo mencionado anteriormente, cuál es el principal problema de seguridad que usted visualiza tanto en su área de trabajo como en el departamento en el cual labora? ¿Por qué?

APÉNDICE E

Estadísticas y Análisis de Resultados

APÉNDICE E: ESTADÍSTICAS Y ANÁLISIS DE RESULTADOS

1. DEPARTAMENTO DE COMPUTACIÓN

Sistema de evaluación para los cuestionarios

Para llevar a cabo el análisis de los cuestionarios realizados para este análisis de riesgo se siguieron los siguientes pasos:

I. Clasificación de las preguntas en secciones de acuerdo con el laboratorio analizado.

II. Asignación de puntos totales a cada sección evaluada en donde cada pregunta cuenta con 3 puntos como máximo valor.

III. Evaluación de las preguntas de cada cuestionario asignando puntos a cada pregunta, en donde:

- 3 puntos = bueno
- 2 puntos =regular
- 1 punto =malo

IV. Conteo de los puntos obtenidos en cada sección.

V. Realización de la gráfica del laboratorio en donde se muestra el porcentaje obtenido en cada sección evaluada con respecto al porcentaje máximo que es el 100%.

VI. Se considera que si se obtiene un 100% en la sección evaluada se tiene una excelente calificación en ese aspecto analizado.

Valorización de preguntas para los laboratorios LINDA, LIDSOL, Laboratorio de computación salas A y B, PROTECO (Tablas E.1, E.2, E.3, E.4 y E.5)

- Cada pregunta del cuestionario equivale a 3 puntos si se obtiene la calificación más alta

Tabla E.1 Evaluación

Control de acceso	3 preguntas	9 puntos totales
Fallas de Software y Hardware	5 preguntas	15 puntos totales
Medidas de seguridad	5 preguntas	15 puntos totales

Tabla E.2 Evaluación Programa de Tecnología en Computación (PROTECO)

Control de acceso físico	5 Puntos
Fallas de Hardware y software	11 Puntos
Medidas de seguridad	9 Puntos

Tabla E.3 Evaluación Laboratorio de Investigación para el Desarrollo Académico (LINDA)

Control de acceso físico	6 Puntos
Fallas de Hardware y software	12 Puntos
Medidas de seguridad	11 Puntos

Tabla E.4 Evaluación Laboratorio de computación salas A y B

Control de acceso físico	9 Puntos
Fallas de Hardware y software	13 Puntos
Medidas de seguridad	11 Puntos

Tabla E.5 Evaluación Laboratorio de Investigación y Desarrollo de Software Libre (LIDSOL)

Control de acceso físico	7 Puntos
Fallas de Hardware y software	11 Puntos
Medidas de seguridad	11 Puntos

Valorización de preguntas para laboratorios: INTEL, y seguridad, Multimedia, Dispositivos lógicos programables, Dispositivos de almacenamiento de entrada y salida, IBM (Tablas E.6, E.7, E.8, E.9 y E.10, E.11, E.12):

Tabla E.6 Evaluación

Control de acceso físico y lógico	18 puntos totales
Hardware y software	27 puntos totales
Mecanismos de seguridad y políticas	27 puntos totales
Seguridad de Redes	6 puntos totales

Tabla E.7 Evaluación Laboratorio de INTEL

Control de acceso físico y lógico	15 puntos
Hardware y software	25 puntos
Mecanismos de seguridad y políticas	18 puntos
Seguridad de Redes	6 puntos

Tabla E.8 Evaluación Laboratorio Multimedia

Control de acceso físico y lógico	15 puntos
Hardware y software	23 puntos
Mecanismos de seguridad y políticas	16 puntos
Seguridad de Redes	3 puntos

Tabla E.9 Evaluación Laboratorio Dispositivos Lógicos Programables

Control de acceso físico y lógico	15 puntos
Hardware y software	23 puntos
Mecanismos de seguridad y políticas	20 puntos
Seguridad de Redes	No aplica

Tabla E.10 Evaluación Laboratorio Dispositivos de Almacenamiento de Entrada y Salida

Control de acceso físico y lógico	15 puntos
Hardware y software	16 puntos
Mecanismos de seguridad y políticas	18 puntos
Seguridad de Redes	No aplica

Tabla E.11 Evaluación Laboratorio IBM

Control de acceso físico y lógico	12 Puntos
Hardware y software	19 Puntos
Mecanismos de seguridad y políticas	20 Puntos
Seguridad de Redes	4 Puntos

Tabla E.12 Evaluación Laboratorio Redes y Seguridad

Control de acceso físico y lógico	17 puntos
Hardware y software	21 puntos
Mecanismos de seguridad y políticas	21 puntos
Seguridad de Redes	1 puntos

Valorización de preguntas para el laboratorio de Microcomputadoras (Tablas E.13, E.14):

Tabla E.13 Evaluación

Control de acceso físico y lógico	12 puntos totales
Hardware y software	18 puntos totales
Mecanismos de seguridad y políticas	30 puntos totales

Tabla E.14 Evaluación Laboratorio de Microcomputadoras:

Control de acceso físico y lógico	10 puntos
Hardware y software	15 puntos
Mecanismos de seguridad y políticas	18 puntos

Valorización de preguntas para cubículos (Tablas E.15, E.16, E.17, E.18, E.19)

Tabla E.15 Evaluación

Control de acceso físico y lógico	3 Puntos totales
Hardware y software	9 Puntos totales
Medidas de seguridad	6 Puntos totales

Tabla E.16 Evaluación Cubículo 1:

Control de acceso físico y lógico	3 Puntos
Hardware y software	9 Puntos
Medidas de seguridad	6 Puntos

Tabla E.17 Evaluación Cubículo 2:

Control de acceso físico y lógico	3 Puntos
Hardware y software	8 Puntos
Medidas de seguridad	6 Puntos

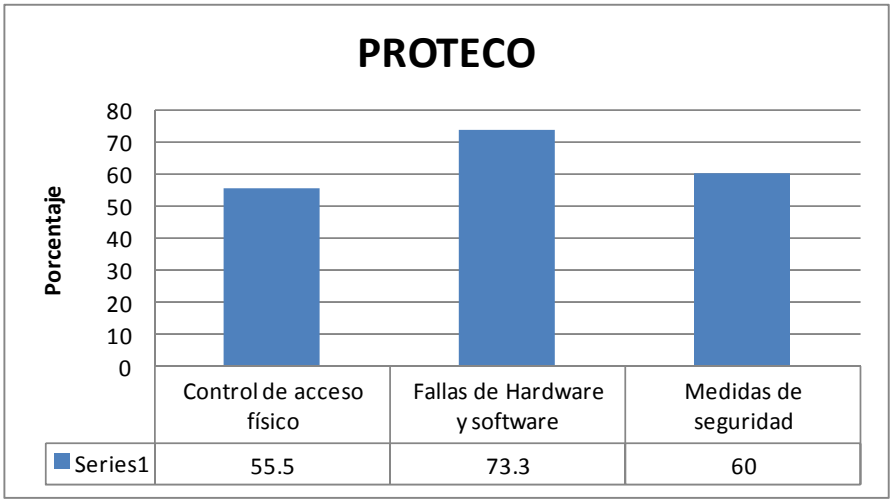
Tabla E.18 Evaluación Cubículo 3:

Control de acceso físico y lógico	3 Puntos
Hardware y software	9 Puntos
Medidas de seguridad	3 Puntos

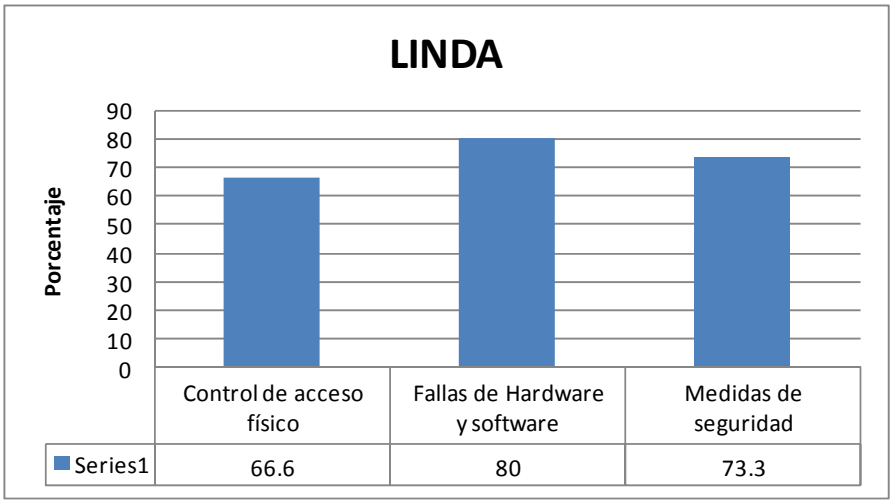
Tabla E.19 Evaluación Cubículo 4:

Control de acceso físico y lógico	2 Puntos
Hardware y software	9 Puntos
Medidas de seguridad	4 Puntos

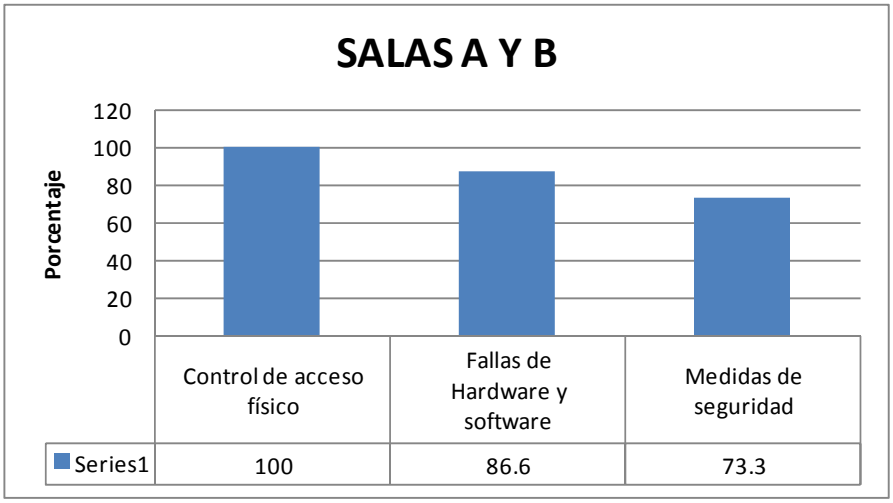
Gráfica E.1 Evaluación PROTECO



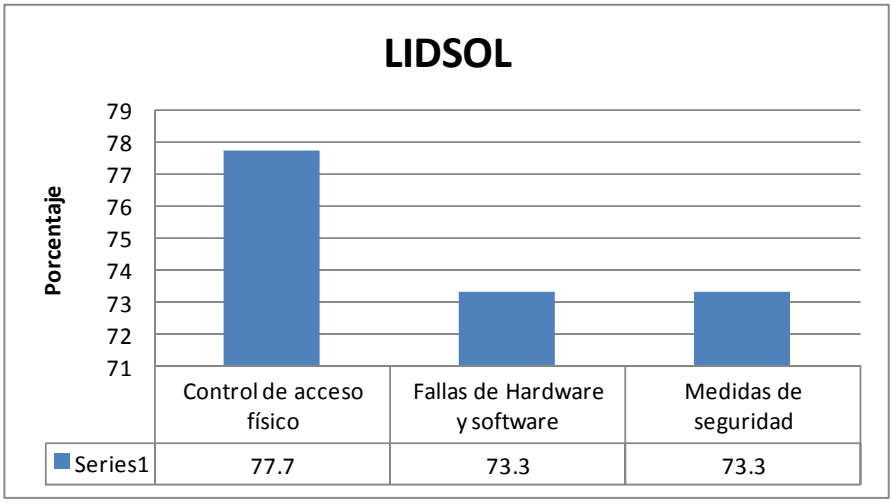
Gráfica E.2 Evaluación LINDA



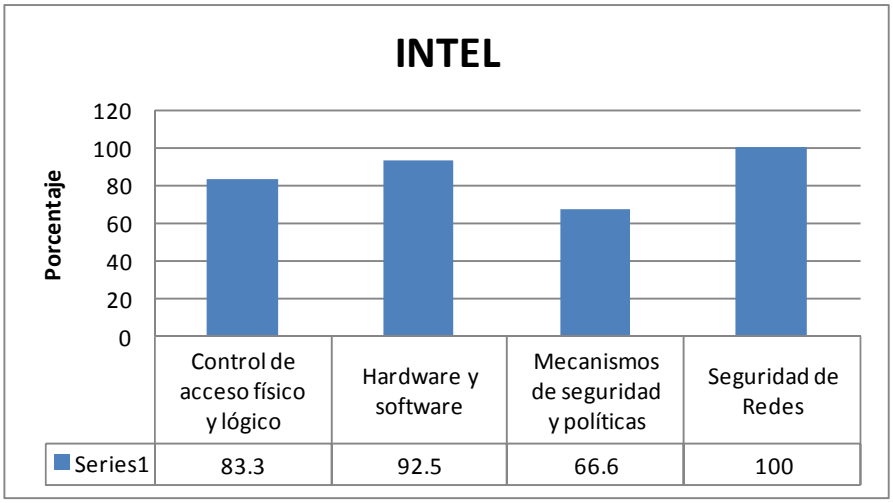
Gráfica E.3 Evaluación Salas A y B



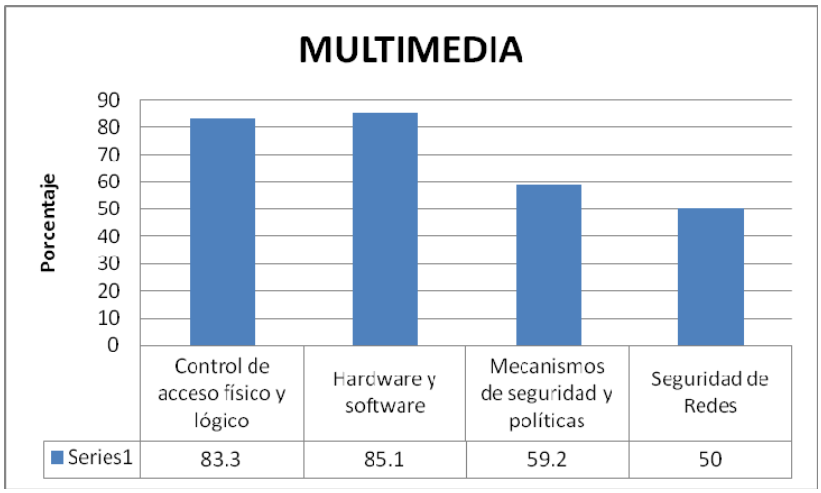
Gráfica E.4 Evaluación LIDSOL



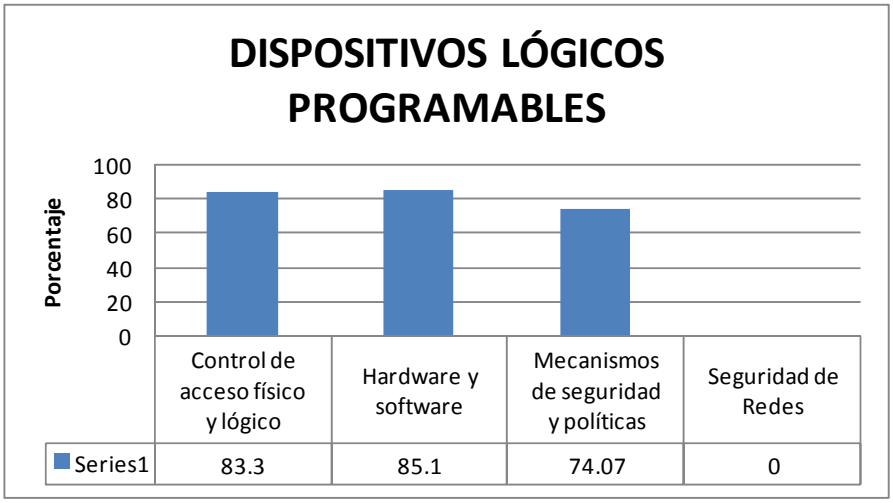
Gráfica E.5 Evaluación INTEL



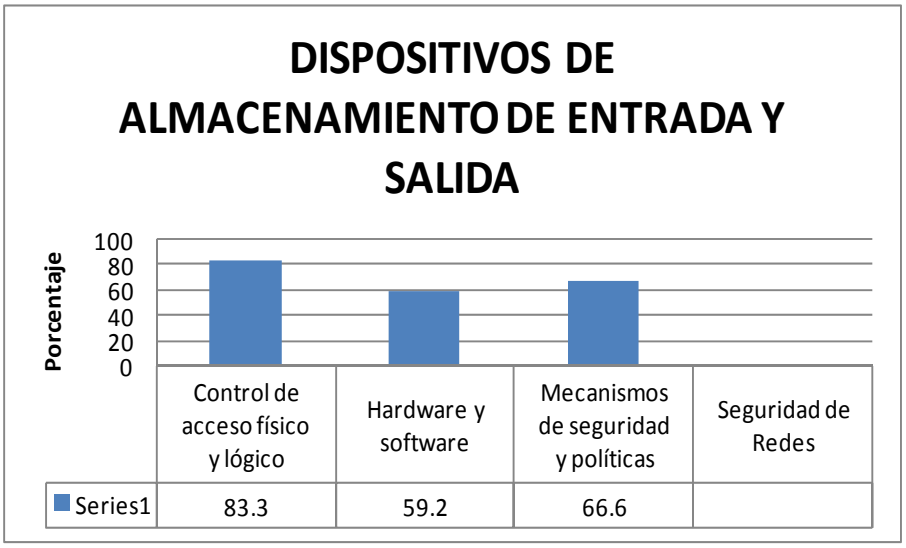
Gráfica E.6 Evaluación Multimedia



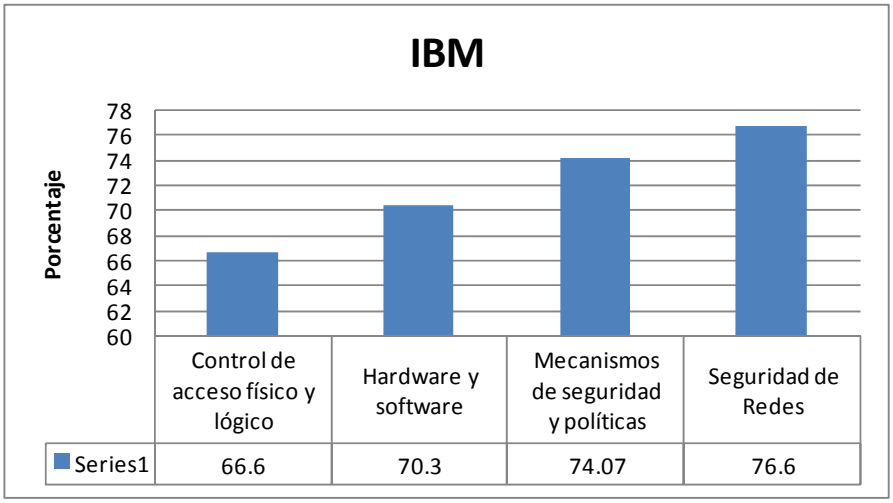
Gráfica E.7 Evaluación Dispositivos Lógicos Programables



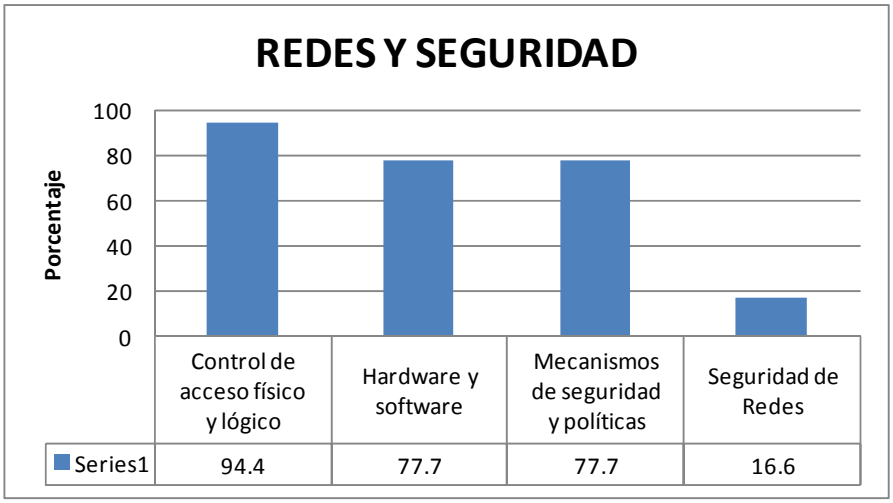
Gráfica E.8 Evaluación Dispositivos de Almacenamiento de Entrada y Salida



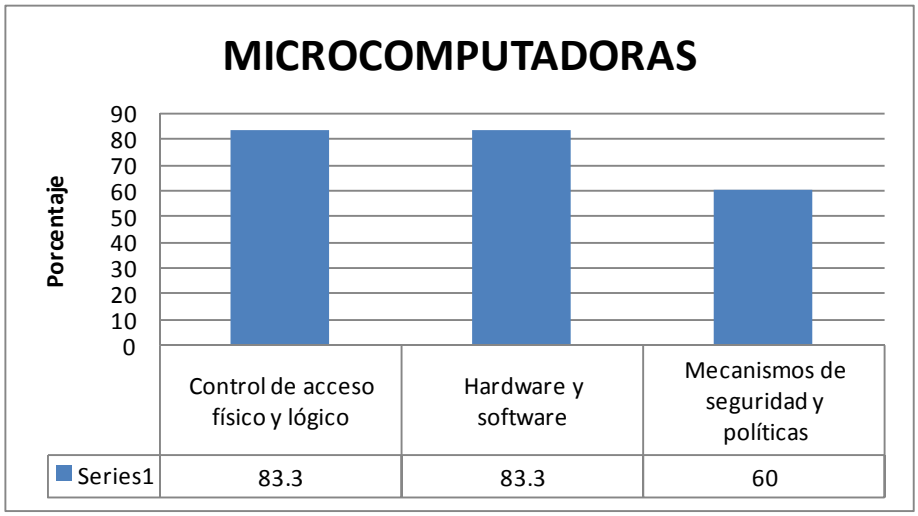
Gráfica E.9 Evaluación IBM



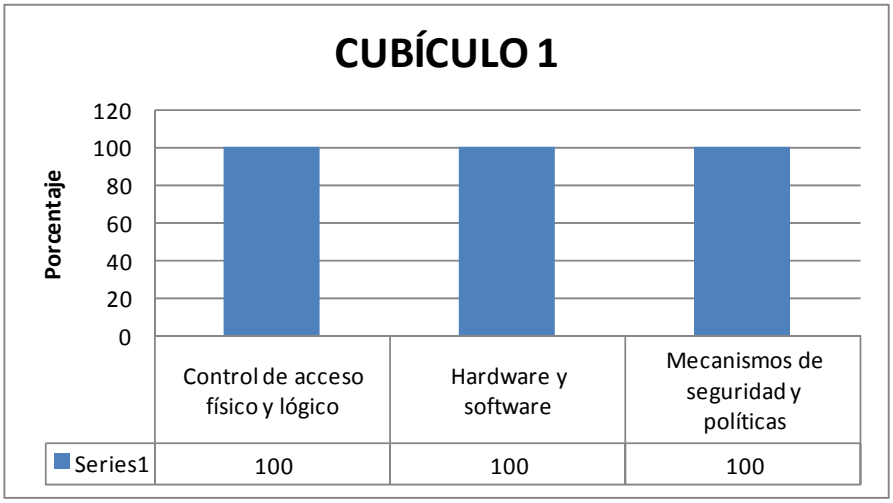
Gráfica E.10 Evaluación Redes y Seguridad



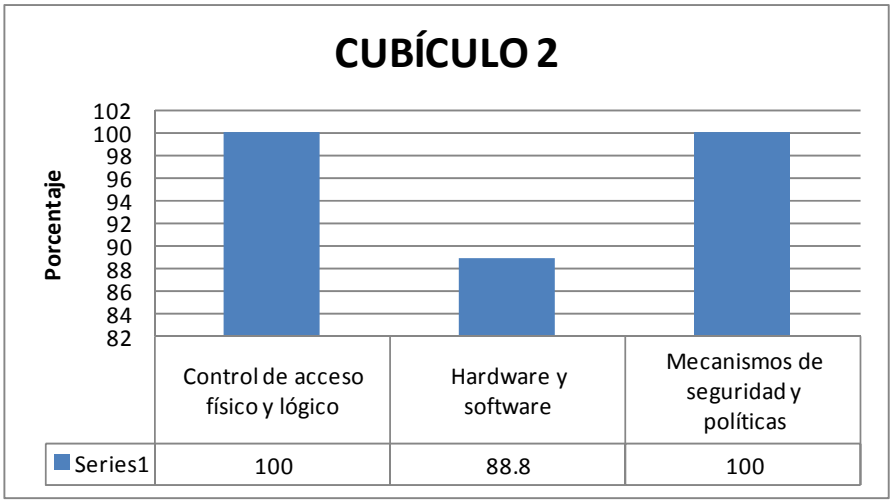
Gráfica E.11 Microcomputadoras



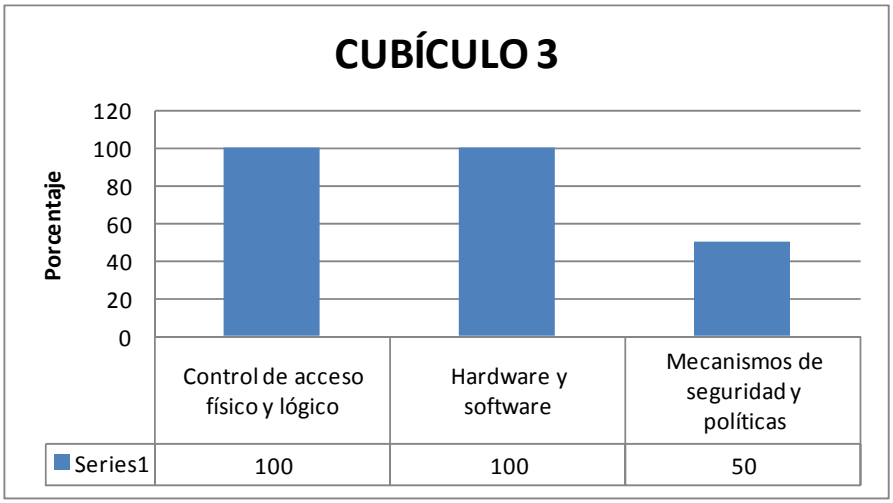
Gráfica E.12 Cubículo 1



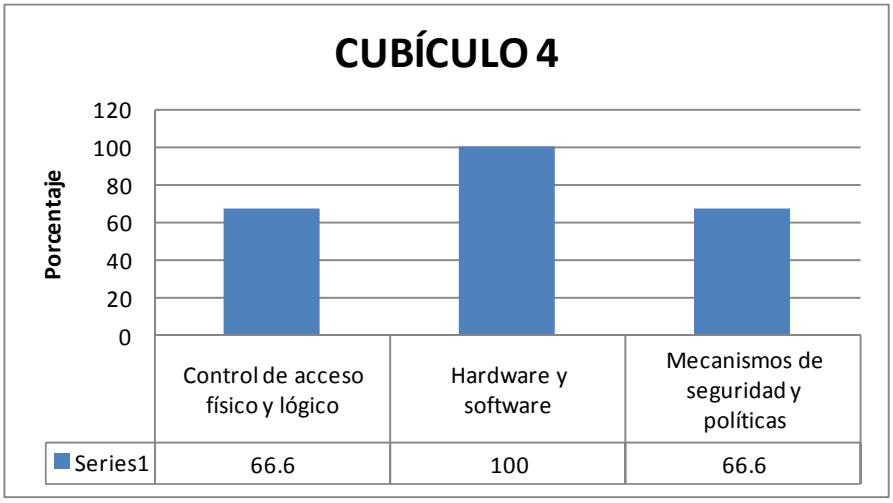
Gráfica E.13 Evaluación Cubículo 2



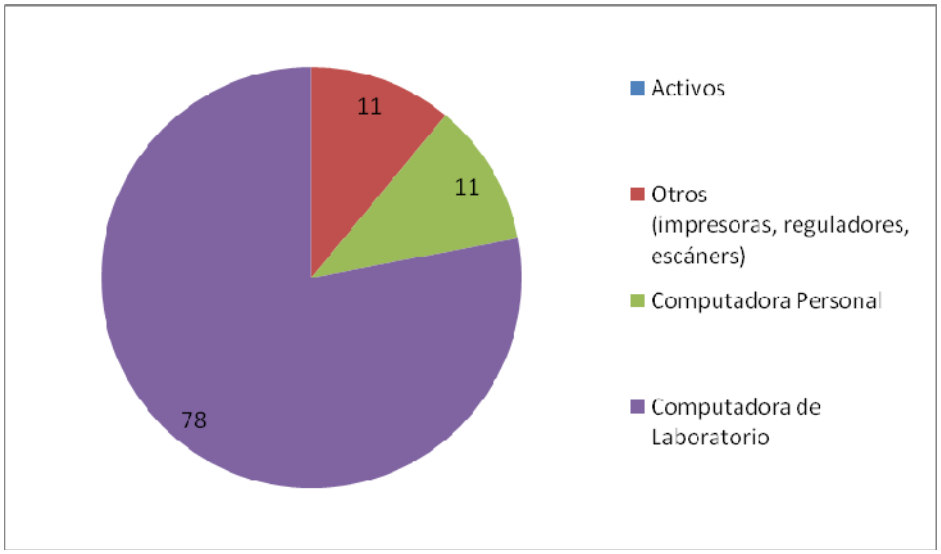
Gráfica E.14 Evaluación Cubículo 3



Gráfica E.15 Evaluación Cubículo 4



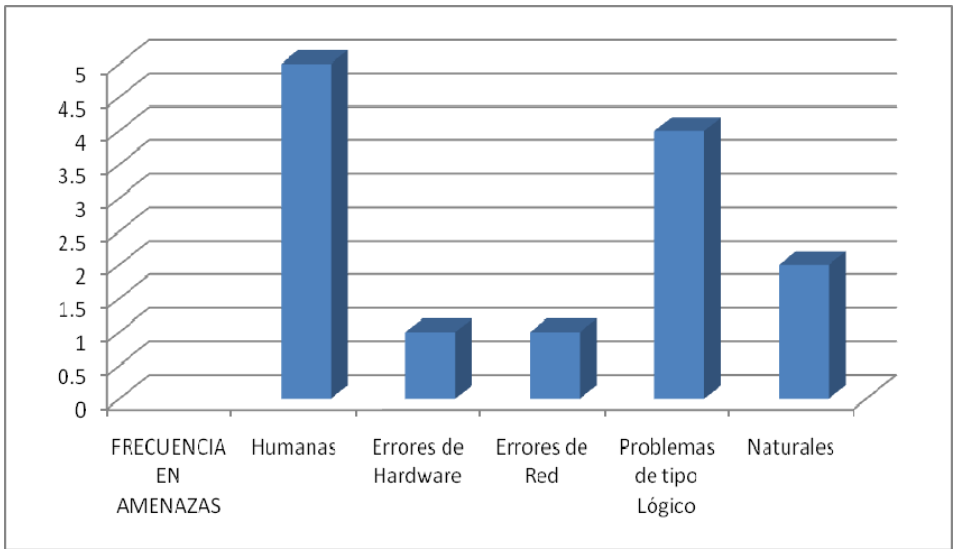
2. DEPARTAMENTO DE CONTROL



Gráfica E.16 Distribución de activos

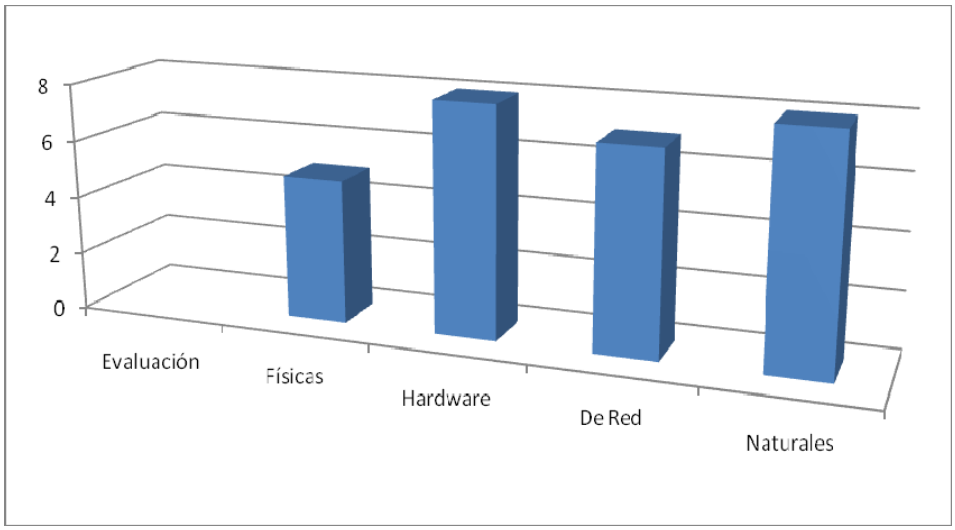
Como se puede observar, el mayor porcentaje de activos comprende a los equipos del laboratorio por lo que las medidas de seguridad en ésta área deberían ser lo más robustas posibles, sin embargo en las siguientes gráficas se puede notar que la seguridad en ésta área en específico deja mucho que desear.

En la siguiente gráfica apreciamos la frecuencia de las amenazas, en donde el número 1 representa una mínima frecuencia y el número 5 representa el valor más alto de ésta.



Gráfica E.17 Frecuencia de Amenazas

En la siguiente gráfica se califica al departamento en cuanto al nivel de seguridad que tienen respecto a las vulnerabilidades que se encontraron. La calificación más alta y la mejor es representada por el número 10.



Gráfica E.18 Evaluación de Vulnerabilidades

COMO SE PUEDE APRECIAR, LA SEGURIDAD FÍSICA ES UN PROBLEMA GRAVE EN ESTE DEPARTAMENTO, YA QUE SU CONTROL DE ACCESO ES NULO Y AL SER EL EQUIPO DE CÓMPUTO EL ACTIVO EN MAYOR CANTIDAD, SE GENERA UN GRAN RIESGO DE PÉRDIDA PARA LA INSTITUCIÓN.

3. DEPARTAMENTO DE ELÉCTRICA DE POTENCIA

ENCUESTA ACERCA DEL CONOCIMIENTO DE LOS VIRUS

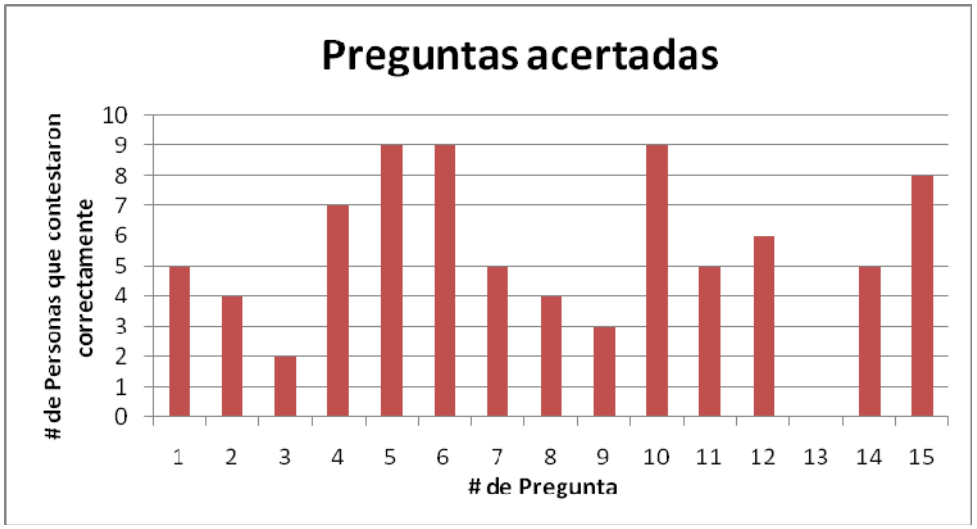
Resultados de la evaluación aplicada al personal que maneja equipo de cómputo en el Departamento de Eléctrica de potencia. Los resultados mostrados a continuación se calificaron con base en las 15 preguntas y descartando o tomando como erróneas aquellas en las que se marcaron dos respuestas de una sola pregunta.

Tabla E.19 Conocimiento de virus

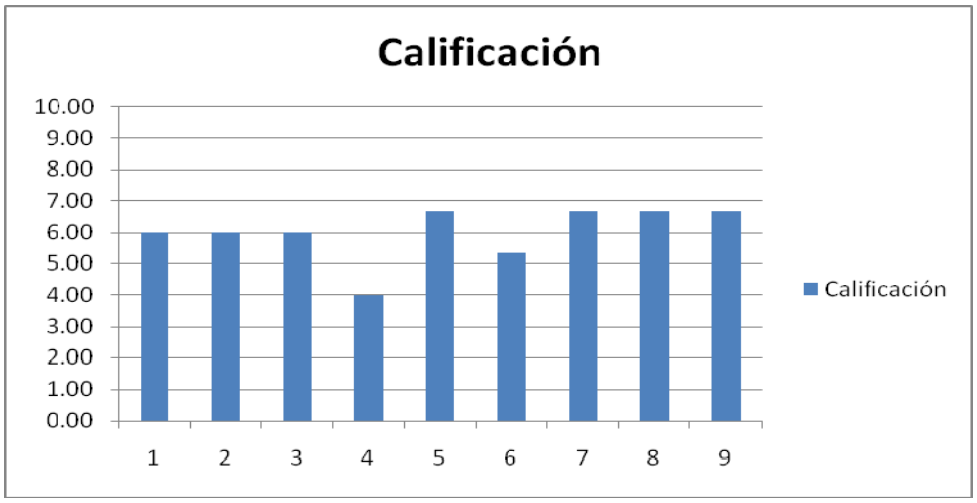
Encuestado	*Puntuación*	*Calificación*
1.	9/15	6
2.	9/15	6
3.	9/15	6
4.	6/15	4
5.	10/15	6.6
6.	8/15	5.3
7.	10/15	6.6
8.	10/15	6.6
9.	10/15	6.6

En las encuestas se puede observar que las personas tienen un conocimiento básico de lo que los virus pueden realizar y de cómo pueden protegerse ante éstos. Gracias a esta encuesta se pudo determinar que debía realizarse un manual con buenas prácticas y difundirlo a todas las personas que utilizan equipos de cómputo.

Los resultados se muestran a continuación (Tablas E.20 y E.21):



Gráfica E.20 Preguntas contestadas correctamente



Gráfica E.21 Calificación

Realmente era necesario realizar un análisis de riesgos del Departamento de Eléctrica de Potencia, ya que al hacer las entrevistas y cuestionarios pertinentes, fue muy obvio que gran parte de las personas que laboran en el departamento desconocen gran parte de las amenazas informáticas que atentan contra su información y activos.

En este departamento no se cuenta con muchos equipos de cómputo, pues la mayoría de ellos están dispersos en cubículos de profesores e investigadores. Solamente cuenta con un laboratorio donde es importante el uso de las computadoras. Por lo que el análisis se enfocó no solo al equipo de cómputo, sino a otro tipo de recursos no informáticos, que no por ello dejan de ser importantes como parte primordial de los activos del departamento o de cada persona que labora en éste.

En lo que se refiere a los conocimientos en el ámbito informático, se detectó que el personal que tiene acceso a una computadora y que cuenta con acceso a Internet no requiere de una amplia gama de servicios, solo lo primordial, y que el conocimiento acerca de qué tipo de daños pueden sufrir a través de este medio es sumamente básico.

De manera general debido al tipo de actividades que se desarrollan en el departamento, se detectó que no se cuenta con un control específico al cual atenerse si se llegase a presentar un problema drástico, el control que se pudo observar fue el que normalmente se lleva en casi cualquier organización, es decir el administrativo.

4. DEPARTAMENTO DE ELECTRÓNICA

Sistema de evaluación para los cuestionarios:

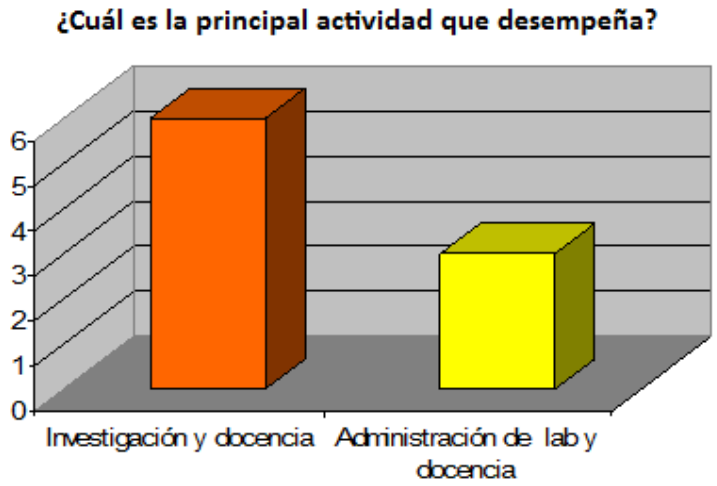
Para llevar a cabo el análisis de los cuestionarios realizados para el análisis de riesgo al departamento de Electrónica, se siguieron los siguientes pasos:

I. Se realizó a los miembros del departamento un cuestionario que consta de catorce preguntas.

II. Se realizaron las graficas de acuerdo con número de personas que se inclinaba más por una respuesta, los encuestados fueron nueve personas.

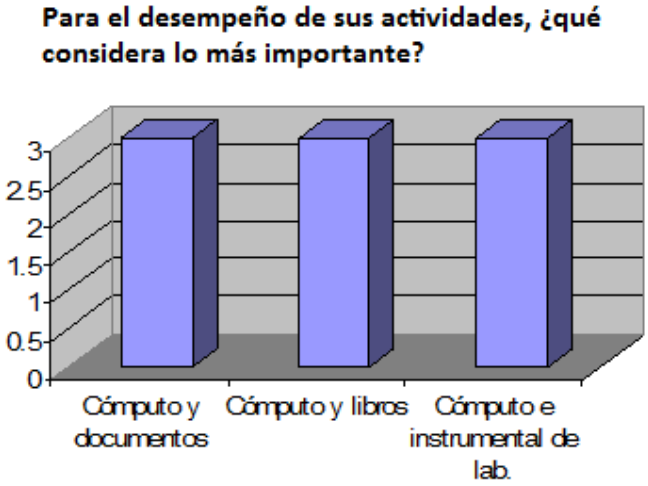
Las gráficas son las siguientes:

Pregunta1.



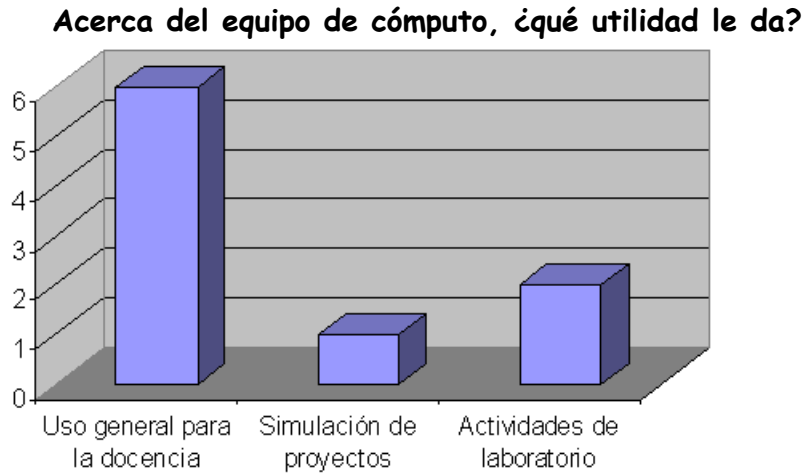
Gráfica E.22 Pregunta 1

Pregunta 2.



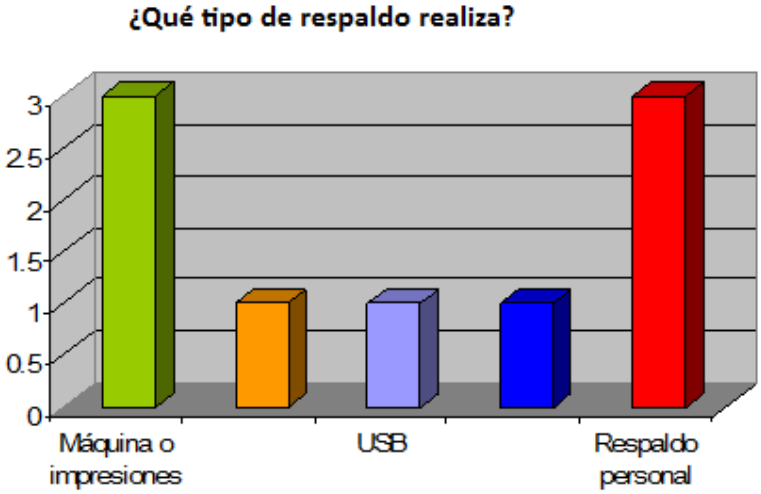
Gráfica E.23 Pregunta 2

Pregunta 3.



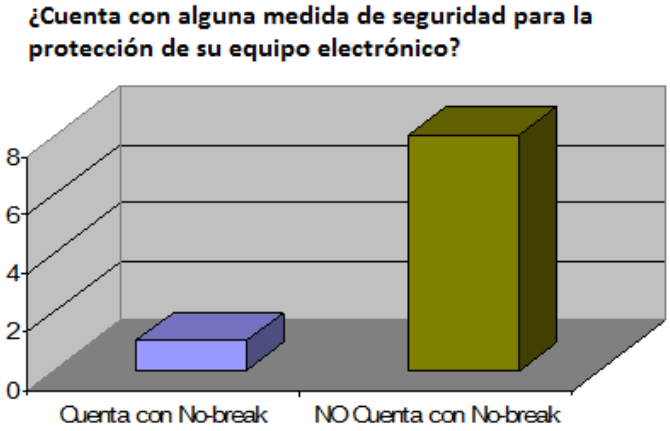
Gráfica E.24 Pregunta 3

Pregunta 4



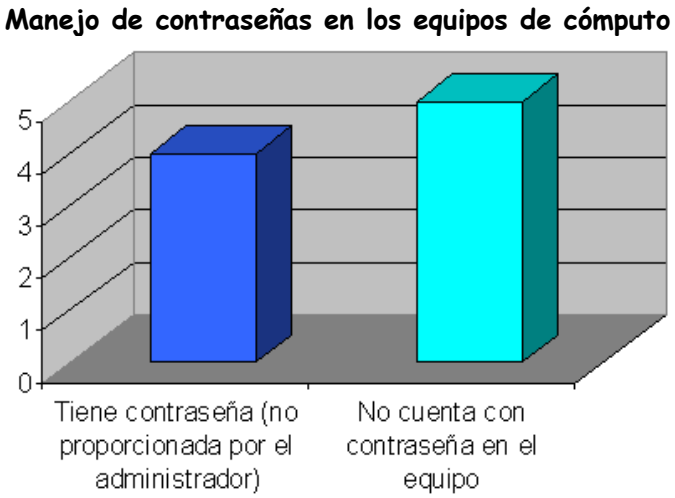
Gráfica E.25 Pregunta 4

Pregunta 5



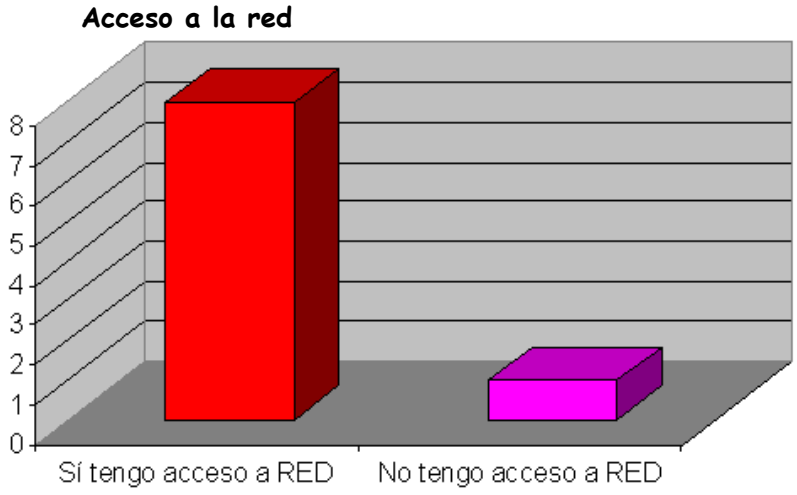
Gráfica E.26 Pregunta 5

Pregunta 6



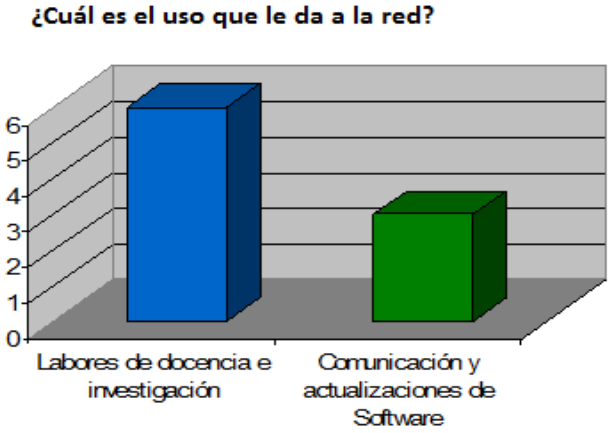
Gráfica E.27 Pregunta 6

Pregunta 7



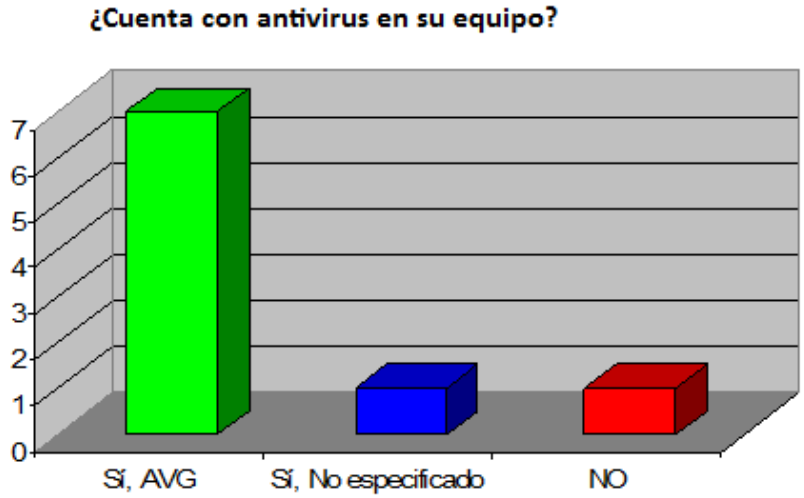
Gráfica E.28 Pregunta 7

Pregunta 8



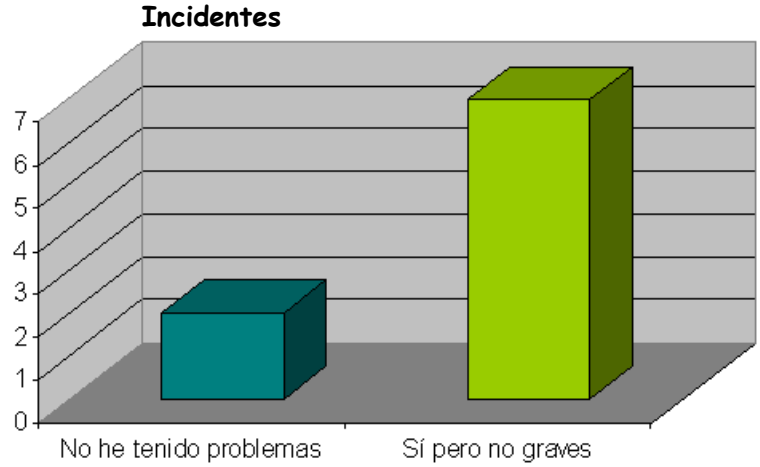
Gráfica E.29 Pregunta 8

Pregunta 9.



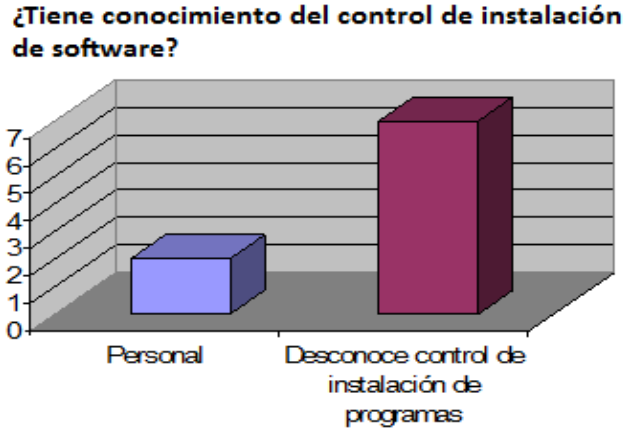
Gráfica E.30 Pregunta 9

Pregunta 10



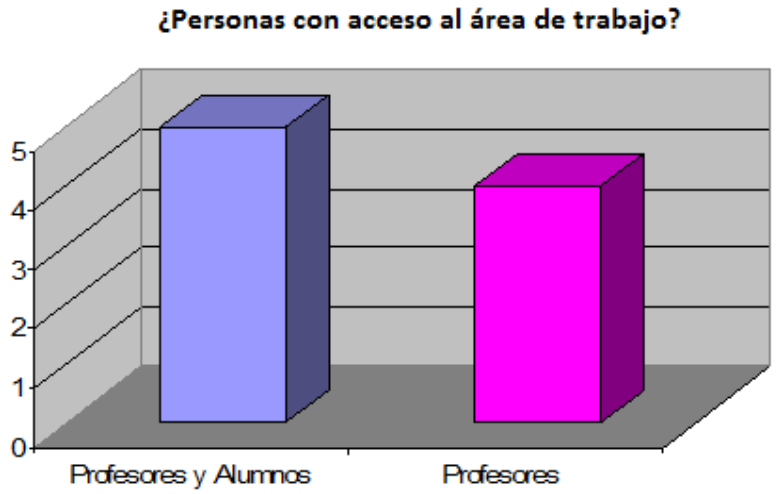
Gráfica E.31 Pregunta 10

Pregunta 11



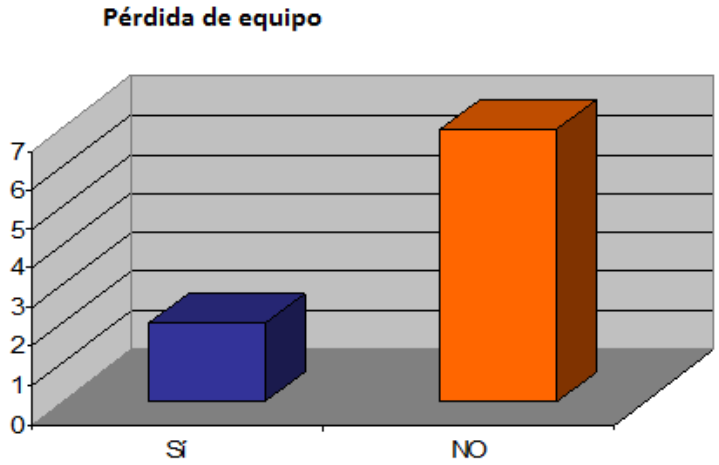
Gráfica E.32 Pregunta 11

Pregunta 12



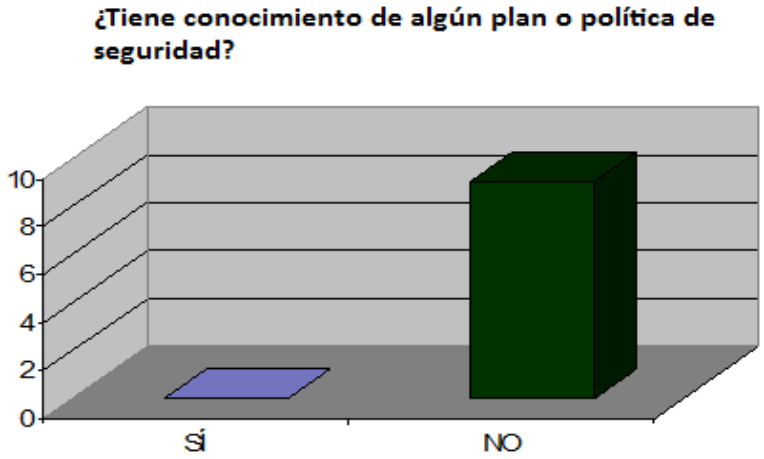
Gráfica E.33 Pregunta 12

Pregunta 13



Gráfica E.34 Pregunta 13

Pregunta 14



Gráfica E.35 Pregunta 14

5. DEPARTAMENTO DE PROCESAMIENTO DE SEÑALES

Se muestran las siguientes gráficas, presentando los resultados obtenidos al realizarse el análisis de Riesgo (Gráficas E36 y E37):

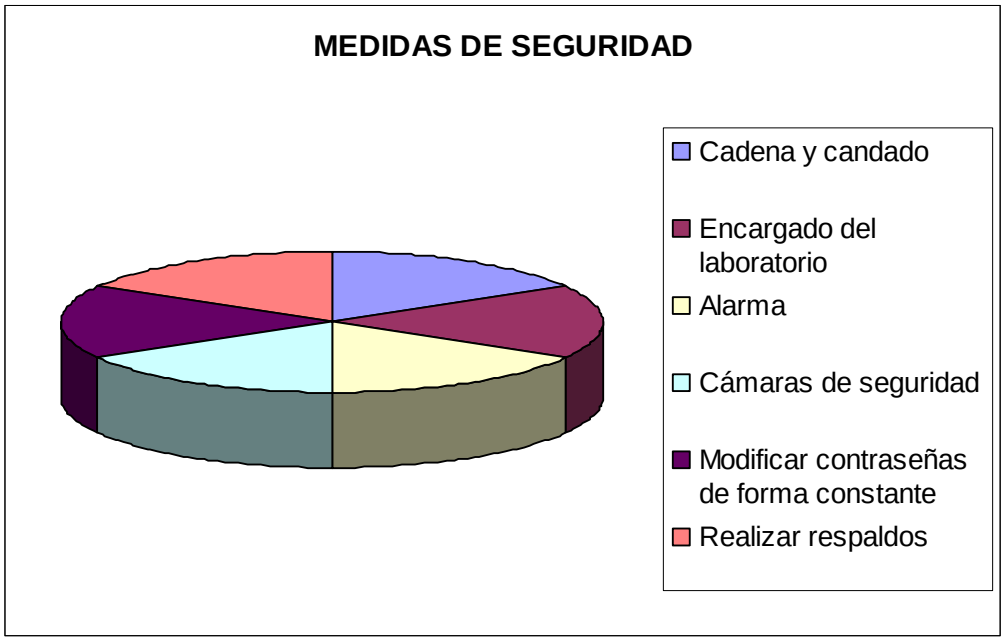


Tabla E.36: Porcentajes del uso de las medidas de seguridad dentro del departamento

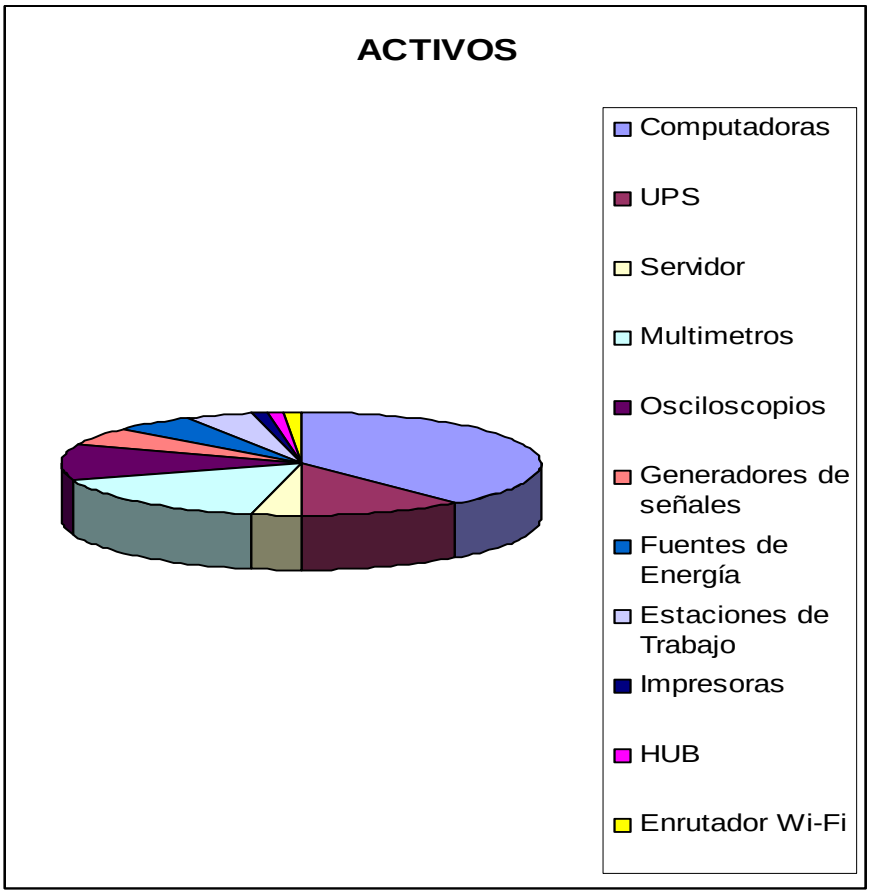
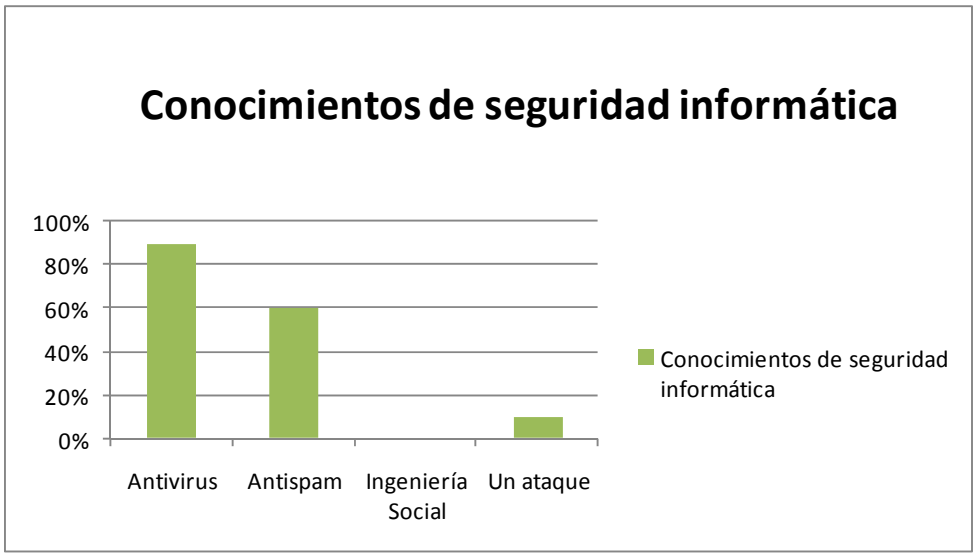


Tabla E.37: Porcentajes de los activos dentro del departamento

6. DEPARTAMENTO DE SISTEMAS ENERGÉTICOS

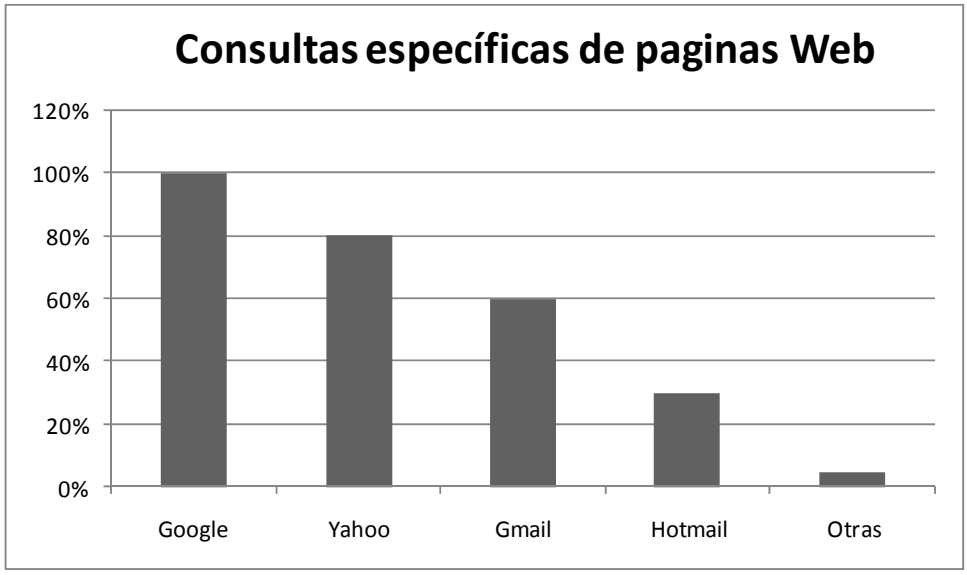
- ¿Sabe qué es un antispam, qué es ingeniería social y qué es un ataque?

  De estas 3 preguntas sólo 5 personas tienen la noción de qué es un antispam, para la pregunta de qué es ingeniería social todos desconocieron el término y finalmente en la última pregunta sólo 1 persona tuvo la noción de qué es un ataque, la gráfica muestra a continuación los porcentajes:



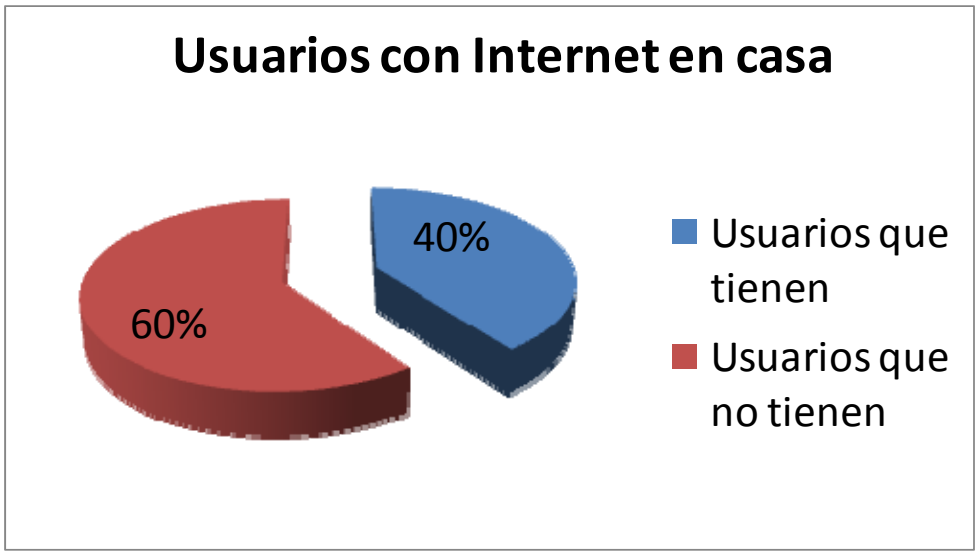
Gráfica E.38 Conocimientos de Seguridad informática

- Las páginas Web más consultadas son: Google, Yahoo, Gmail y Hotmail

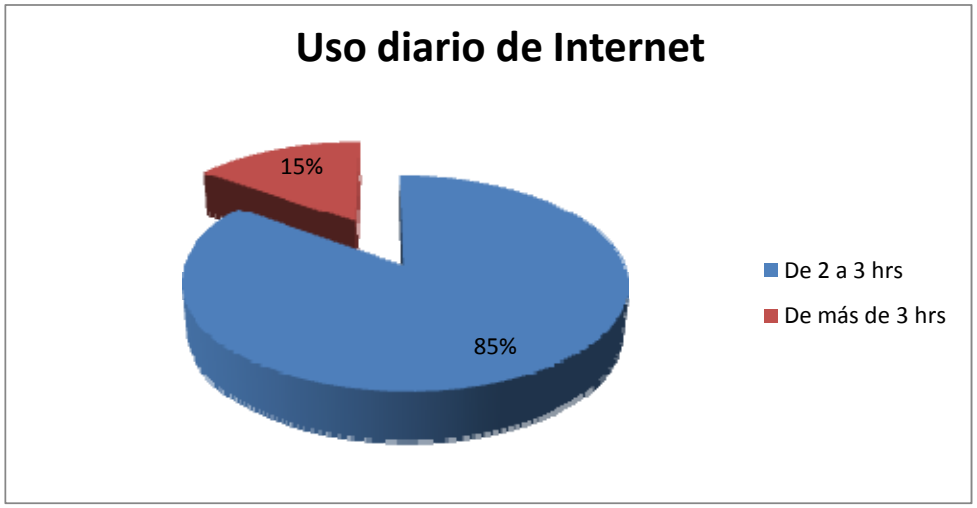


Gráfica E.39 Consultas específicas de páginas web

- La mayoría de los usuarios trabaja de 2 a 3 horas diarias en Internet, y sólo 4 tienen conexión de internet en casa.



Gráfica E.40 Usuarios con internet en casa



Gráfica E.41 Uso diario de internet

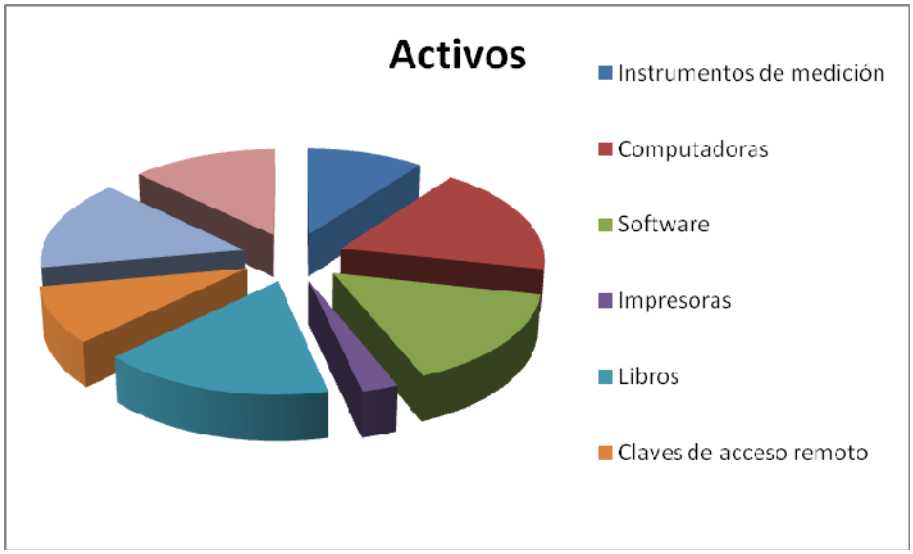
- Los usuarios comentan que no tienen problemas con la conexión de internet del Departamento de Sistemas Energéticos, además se han quedado sin servicio de Internet, pero previamente se les comunicó y por otro lado, es muy raro que hayan tenido un problema con la luz y en su momento cuentan con un no-break.

- Sólo 3 usuarios han bajado música de Internet y 7 se han infectado al descargar algún programa o archivo.

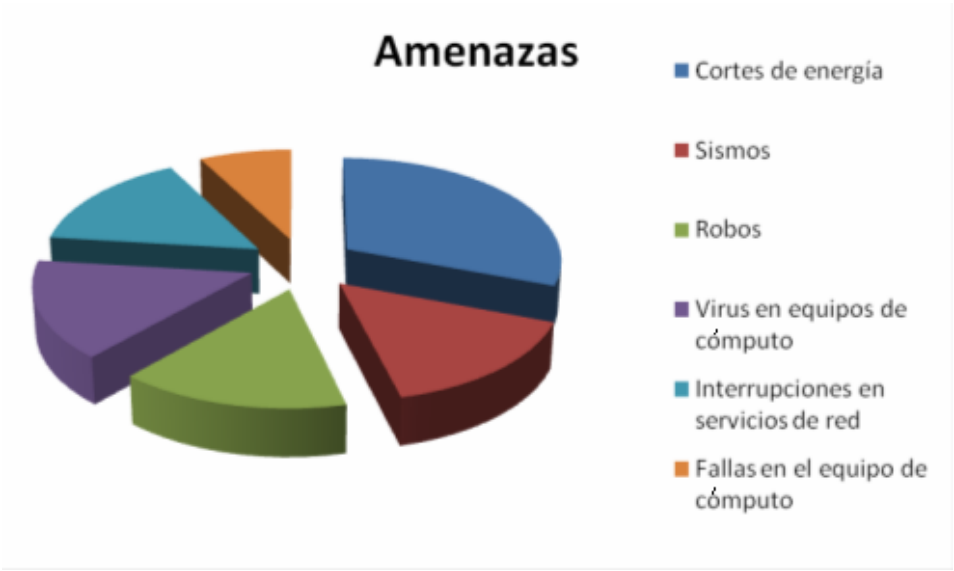
- Todos los usuarios hacen y cuentan con respaldos de su información lo que demuestra que cuidan su información.

7. DEPARTAMENTO DE TELECOMUNICACIONES

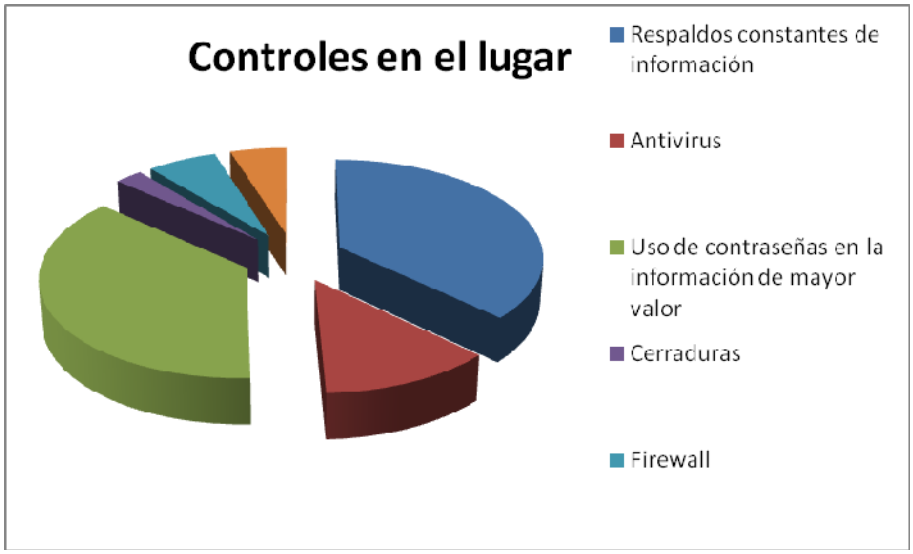
A continuación se muestran las gráficas E.42, E.43 y E.44 del análisis de Riesgo.



Gráfica E.42 Identificación de activos



Gráfica E.43 Identificación de las amenazas.



Gráfica E.44 Porcentaje de controles que se tienen en el Departamento.

Como se puede observar en la gráfica, el aspecto de seguridad física en cuanto a cerraduras y control de acceso es prácticamente nulo por lo que las amenazas en ese sentido pueden ser más abundantes.

Lo anterior toma mayor importancia al poder ver en las primeras dos gráficas que el mayor porcentaje de activos está concentrado en equipo y que el mayor porcentaje de amenazas tiene que ver con el robo de éste; por lo que es determinante reforzar la seguridad física en el departamento.

REFERENCIAS

REFERENCIAS

- Análisis de riesgo (Última revisión 09-Enero-2009)

  http://info-resumendeseguridad.blogspot.com/2007/12/anlisis-de-riesgos-y-vulnerabilidades.html

- Análisis de riesgo (Última revisión 09-Enero-2009)

  http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsechtml/node334.html

- Análisis de Riesgos (Última revisión 20-abril-2009)

  http://www.rediris.es/cert/doc/unixsec/node31.html

- Análisis de Riesgo Departamento de Control (Última revisión 7-mayo-2009)
  http://www.mtas.es/insht/monitor/ST/v/stv08.pdf

- Análisis de Riesgo Departamento de Control (Última revisión 7-mayo-2009)

  http://www.unizar.es/guiar/1/Accident/An_riesgo/An_riesgo.htm#Met_general

- Análisis Forense (Última revisión 26-abril-2009)

  http://www.ausejo.net/seguridad/forense.htm

- Apuntes de la asignatura Seguridad Informática I, impartida por la profesora M.C. Cintia Reyes Quezada, Facultad de Ingeniería, UNAM, Semestre 2008-1

- Conceptos Básicos de Seguridad Informática (Última revisión 1-abril-2009)

  www.eurologic.es/conceptos/conbasics.htm

- Fundamentos de Seguridad Informática (Última revisión 20-marzo-2009)

  http://www.hackstudio.net/hackLabs/NKTHack1.html

- Glosario (Última revisión 5-mayo-2009)

  http://es.wikipedia.org/wiki/Procesador_digital_de_se%C3%B1al

- Glosario (Última revisión 5-mayo-2009)

  http://es.wikipedia.org/wiki/SAI

- Herramientas de Seguridad Informática (Última revisión 05-Diciembre-2008)

  http://www.masadelante.com/faq-cortafuegos.htm

- Herramientas de Seguridad Informática (Última revisión 02-Enero-2009)

  http://www.alegsa.com.ar/Notas/261.php

- Herramientas de Seguridad Informática (Última revisión 02-Enero-2009)

  http://es.kioskea.net/contents/attaques/balayage-ports.php3

- Herramientas de Seguridad Informática (Última revisión 02-Enero-2009)

  http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

- Herramientas de Seguridad Informática (Última revisión 09-Enero-2009)

  http://sitescope.tellurian.net/SiteScope/docs/LogFileMon.htm

- Herramientas de Seguridad Informática (Última revisión 09-Enero-2009)

  http://www.seguridadenlared.org/es/index25esp.html

- Herramientas de Seguridad Informática (Última revisión 11-Enero-2009)

  http://vtroger.blogspot.com/2008/05/anlisis-forense-de-accesos-no.html

- Herramientas de Seguridad Informática (Última revisión 11-Enero-2009)

  http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=4&pagina=2

- Herramientas de Seguridad Informática (Última revisión 11-Enero-2009)

  http://www.monografias.com/trabajos43/seguridad-redes/seguridad-redes2.shtml#medidas

- Herramientas de Seguridad Informática (Última revisión 11-Enero-2009)

  http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGSO00.htm

- Herramientas de Seguridad Informática (Última revisión 11-Enero-2009)

  http://www.saulo.net/pub/inv/SegWiFi-art.htm

- Herramientas de Seguridad Informática (Última revisión 11-Enero-2009)

  http://mmc.geofisica.unam.mx/LuCAS/Presentaciones/200103hispalinux/ferrer/html/sistema-operativo.html

- López B. María Jaquelina y Quezada R. Cintia. *Fundamentos de seguridad informática.* México, UNAM, Facultad de Ingeniería, 2006.
- Sensores Biométricos. (Última revisión 20-abril-2009)

  www.ibia.org
- Servicios de Seguridad (Última revisión 2-Diciembre-2008)

  http://www.segu-info.com.ar/logica/identificacion.htm
- Servicios de Seguridad (Última revisión 06-Enero-2009)

  http://www.segu-info.com.ar/logica/identificacion.htm
- Servicios de Seguridad (Última revisión 10-Enero-2009)

  http://www.iec.csic.es/criptonomicon/seguridad/servicio.html
- Servicios de seguridad (Última revisión 10-abril-2009)

  http://www.delitosinformaticos.com/especial/seguridad/servicios.shtml