UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE INGENIERÍA ELÉCTRICA

PROPUESTA DE APLICACIÓN DE UNA METODOLOGÍA PARA LA SEGURIDAD INFORMÁTICA EN LA DIVISIÓN DE CIENCIAS BÁSICAS

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

GAÍNZA SÁNCHEZ SABINO ISAO

DIRECTORA DE TESIS:

VALDEZ Y ALFARO IRENE PATRICIA

MÉXICO, D.F. 2009

- *A la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, por haberme otorgado una formación integral.*

- *A la División de Ciencias Básicas, por haberme permitido colaborar en el área de cómputo y realizar esta tesis.*

- *A mi familia y amigos. por el apoyo que me han dado.*

- *A Irene Patricia Valdez y Alfaro, por su enorme apoyo en la realización de esta tesis.*

- *A Cecilia Teresa Carmona Téllez, por la co-dirección de este trabajo de tesis y sus valiosas aportaciones.*

ÍNDICE

PROBLEMÁTICA

El concepto de seguridad de la información implica un conjunto de metodologías, mecanismos, herramientas, procedimientos y buenas prácticas, que buscan el aseguramiento de recursos informáticos, como la información misma, datos, usuarios, equipos y dispositivos. La seguridad no es un producto, es un proceso. Un sistema de información es tan seguro, como lo es el eslabón más débil.

Un equipo nunca podrá encontrarse protegido en un 100%, es decir, por más esfuerzos que se realicen por asegurarlo, siempre existirá un pequeño resquicio que pueda comprometerlo. Por lo que se busca es tener una aproximación lo más cercana posible.

Actualmente la seguridad es de suma importancia y ha tenido grandes avances en los últimos años, ya que existe una mejor concientización de las empresas debido a los diversos peligros a los que se enfrentan. Sin embargo, a nivel de usuarios finales, la seguridad se encuentra en general en un nivel de total desconocimiento y sólo se le pone el énfasis debido en determinadas ocasiones, como en el uso de comercio electrónico (aunque muchas veces los esfuerzos son insuficientes).

La seguridad es una carrera continua y consistente entre los atacantes y los administradores de los sistemas. Mientras un atacante sólo tiene que aprovechar una única vulnerabilidad para lograr alcanzar una penetración, un administrador tiene que blindarlo en contra de todas las vulnerabilidades posibles en su contra, ya sean conocidas o por conocer. Debido al actual estado de democratización del conocimiento (la información se encuentra accesible), prácticamente cualquier individuo puede provocar un incidente, ya sea haciendo sus propios programas o utilizando algunos que se encuentran disponibles a través de Internet.

La implantación de la seguridad usualmente colisiona con la eficiencia. No es prudente colocar varios controles o mecanismos que protejan la información, si éstos vuelven ineficientes los procesos o procedimientos que hagan uso de ella. También habrá que cumplir el principio de proporcionalidad, de que el costo de implantar controles que busquen proteger cierta información no debe ser mayor al costo de la información misma, o al costo en caso de pérdida o divulgación.

Al no contar con un nivel de seguridad aceptable, una organización está expuesta a una serie de incidentes que podrían comprometer seriamente su misión. Las repercusiones pueden ir desde una corta denegación de servicios, divulgación de información sensible, pérdida de reputación, hasta la quiebra total.

Actualmente las motivaciones de los atacantes han cambiado radicalmente, antes un atacante buscaba prestigio y notoriedad, además de que representaba demostrar que será mejor que los administradores o encargados de la seguridad y en ocasiones se podía tomar como un juego (estar siempre un paso por delante). Sin embargo, ahora se han profesionalizado grupos de hackers que enfocan sus esfuerzos en comprometer sistemas en busca de obtener ganancias económicas, es decir, la gran motivación actual es monetaria.

Existen ciertas organizaciones que llevan a cabo estudios de actividades relacionadas con la seguridad, con el fin de poder observar ciertas tendencias en su comportamiento. Existen dos que son los más notorios: el *CSI Computer Crime and Security Survey* elaborado por el Computer Security Institute y el *Data Breach Investigations Report* elaborado por Verizon.

La CSI Survey, es la encuesta más referenciada en estudios de seguridad. Se realiza aleatoriamente, pero sobre la población perteneciente a la comunidad CSI, que trabaja activamente en el mejoramiento de la seguridad, es decir, se trata de empresas que tienen por lo menos el mínimo grado de concientización acerca de la seguridad. Un 65% de los que respondieron la encuesta del 2008, cuentan con puestos que se dedican a tiempo completo a la seguridad en sus empresas.

El CSI arrojó que más de la mitad de las empresas encuestadas invierte en seguridad tan sólo el 5% del total del presupuesto dedicado a las Tecnologías de la Información (TI). El 46% aceptó haber experimentado incidentes de seguridad, y un 10% no sabe si tuvo alguno, por lo que se pueden contabilizar como posibles. También se observó que en el 2008 la mitad de los incidentes se produjeron por personal dentro de las empresas. Arroja que los incidentes más comunes involucran virus (50% del total de empresas reportaron incidentes), abuso de usuarios internos (44%), robo de laptops (42%), accesos no autorizados (29%), denegación de servicios (21%), abuso de mensajería instantánea (21%), y bots (20%); mientras que incidentes relacionados a abuso de redes inalámbricas, penetración a sistemas, fraude financiero, mal uso de aplicaciones web, robo de contraseñas, ataques a DNS, robo o pérdida de información de clientes, web defacement, robo o pérdida de información propietaria, fraudes en

telecomunicaciones y sabotaje tuvieron tan sólo 14% o menos de ocurrencia; reportando una pérdida por incidentes en promedio de alrededor de 300 000 dólares, y se detectó que el incidente que más se repitió, los virus, tan sólo tuvo un promedio de 40 000 dólares en pérdidas. Una de cada cuatro empresas lograron detectar ataques específicamente dirigidos, por lo que estos ataques son más sofisticados y mucho más difíciles de detectar y mitigar.

En el reporte de Verizon del mismo año se observa que el código malicioso utilizado en distintos ataques es comúnmente plantado por los atacantes (58%), mientras que el código que es colocado mediante correo, propagación en redes y vía web son también utilizados constantemente (13% cada uno) y la instalación física de éste no es una técnica utilizada realmente (2%).

También se muestra que los ataques dirigidos tan sólo constituyen un 15%, mientras que los ataques oportunistas son los que más imperan, de éstos la mitad son totalmente aleatorios y la otra mitad el objetivo fue seleccionado por habérsele conocido una vulnerabilidad que el atacante pudiera explotar.

Arroja también que el tiempo desde que el atacante penetra un sistema hasta que logra comprometerlo la mayoría de las veces en tan sólo minutos, mientras que el tiempo en que se descubre que el sistema ha sido comprometido puede llegar hasta varios meses, y el tiempo desde que se descubre el compromiso, hasta que se mitiga el impacto usualmente está en el orden de semanas.

En cuanto a ataques vía web, la vulnerabilidad más utilizada en los ataques, es la inyección SQL, mientras que otras como el cross site scripting, autenticación y anti-automatización insuficiente, son utilizadas en conjunto tan sólo en uno de cada cinco incidentes.

Las tendencias a observar son:

- Los volúmenes de ataques con origen en otras naciones (principalmente desde China) aumentan, especialmente dirigidos a redes gubernamentales y militares.
- Incidentes relacionados a robo de datos aumentan debido a la facilidad de acceso a dispositivos móviles.
- Los ataques a nivel de aplicación como inyección SQL, buffer overflows y cross site scripting aumentan en sofisticación debido a que son dirigidos a sitios con mucho tráfico, como redes

sociales o de noticias, que si llegaran a ser comprometidos, podrían alcanzar un gran número de usuarios.

- La mayoría de los ataques no son de una gran complejidad y pueden ser aminorados con controles sencillos.

DEFINICIÓN DEL PROBLEMA

La DCB se rige mediante las políticas de seguridad de la FI publicadas desde el año 2003, aunque hace falta mayor difusión de las mismas entre su comunidad. Se cuentan con esfuerzos que buscan mitigar los riesgos identificados de manera empírica, como la amplia distribución y utilización de software antivirus, la utilización de firewalls en ciertas áreas, cierta documentación de procedimientos (más orientado a fines administrativos), utilización de contraseñas robustas para determinados servicios, utilización de grupos para otorgar privilegios a usuarios en distintos sistemas y aplicación de parches y actualizaciones. A su vez, se cuenta con políticas de seguridad internas dentro de cada área de cómputo pero que no se encuentran respaldadas pos algún documento oficial avalado por las autoridades de la misma División.

Se cuenta con un nivel de seguridad que no es el óptimo, existen ciertos problemas relacionados con la seguridad que deben de ser corregidos como la elaboración de políticas de seguridad propias y actuales, no se tiene un panorama certero de la situación de seguridad en la División, no se cuenta con documentación en caso de incidentes, planes de respuesta a desastres en áreas críticas o procedimientos. No hay procedimientos que definan la periodicidad con la que se deben realizar respaldos de información o aplicaciones. No se tienen identificadas las vulnerabilidades que podrían ser utilizadas para afectar el correcto funcionamiento tanto de la red, como de los sistemas de información. Tampoco se tiene clasificada ni la información ni los usuarios, de acuerdo a su nivel crítico o sensibilidad.

Se han suscitado distintos incidentes de seguridad que podrían ser disminuidos o eliminados con la implantación de ciertos controles de seguridad.

Tampoco se cuenta con ningún estudio anterior aplicado a la DCB relacionado a la seguridad de la información que sirva de apoyo en la toma de decisiones relacionadas con el equipo de cómputo.

Por todo esto, se hace necesaria la elaboración de un estudio que abarque la totalidad de la infraestructura de cómputo de la DCB.

OBJETIVO

Elaborar un estudio de gestión de riesgos que permita obtener una propuesta fundamentada de los controles de seguridad adecuados que se requieran implantar en la DCB con el fin de mitigar los riesgos identificados.

Documentar los aspectos de seguridad más relevantes referentes al cómputo en la DCB que sirva como marco de referencia para trabajos posteriores.

ALCANCE

Este trabajo abarca todos los sistemas de información, la red de datos que soporta al equipo de cómputo en los edificios del Ala Poniente, de la Torre, laboratorios y jefatura de la División de Ciencias Básicas (DCB) de la Facultad de Ingeniería (FI) de la UNAM.

No se harán observaciones en cuanto a la seguridad física, por cuestiones administrativas y separación de funciones existentes en la Universidad.

También comprende a las entidades (usuarios, procesos y dispositivos) que forman parte de la División, y el papel que deberán jugar en dicha propuesta. Asimismo, se estudiará la normatividad existente y se propondrán cambios a la documentación y procedimientos o en su defecto, la creación de nuevos.

ANTECEDENTES DE LA DCB

La División de Ciencias Básicas es una de las seis divisiones académicas de la Facultad de Ingeniería, su tarea fundamental es impartir las asignaturas de las ciencias básicas de las doce carreras que se imparten en la FI de la Universidad Nacional Autónoma de México.

MISIÓN

"Coadyuvar a la formación integral y sólida de los alumnos de la Facultad, proporcionándoles los conocimientos de matemáticas, física y química necesarios para continuar en forma exitosa sus estudios de licenciatura; inculcarles valores éticos, conciencia social y ecológica, espíritu crítico, asertividad, liderazgo y deseos de aprender de manera permanente por sí mismos al valorar la riqueza de sus nuevos conocimientos; fomentar la colaboración del trabajo en equipo, la adquisición de aptitudes, actitudes y valores necesarios para que sean ingenieros reconocidos nacional e internacionalmente como verdaderos agentes promotores de cambio y beneficio social congruentes con el espíritu de nuestra universidad.

Lograr que su personal académico esté actualizado en el conocimiento de sus asignaturas y en las habilidades, actitudes y valores que debe ejercer y practicar ante sus alumnos; de manera tal que se gane el respeto, la admiración y el cariño de éstos y se constituya en ejemplo a seguir por sus alumnos; mediante el uso de las metodologías pedagógicas de apoyo al aprendizaje, a la formación de equipos de trabajo en el grupo, la orientación y guía; la utilización de apoyos didácticos y computacionales que favorezcan el aprendizaje y la realización de actividades que promuevan la reflexión de los valores éticos que fortalecen el espíritu humano y la sana convivencia social.

Fortalecer los vínculos con las demás Divisiones de la Facultad para conocer sobre sus problemas sobre ciencias básicas, con el bachillerato de la UNAM para coadyuvar a que los alumnos que ingresan a la Facultad de este subsistema traigan los antecedentes de ciencias básicas requeridos, vocación sólida sobre la ingeniería y hábitos de estudio, para mitigar la reprobación y la deserción que históricamente se da en los primeros semestres, y con las demás dependencias universitarias y universidades nacionales e internacionales para mantener actualizados los contenidos de las matemáticas y las ciencias básicas, mejorar las prácticas docentes de las mismas; así como difundir nuestros avances y novedades académicas y acrecentar el conocimiento universal."

VISIÓN

"En consonancia con la visión de la Facultad de Ingeniería, la División de Ciencias Básicas (DCB) de esta Facultad es moderna, dinámica y vanguardista. Su calidad continuamente certificada en todos los procesos y su nivel académico compiten con los de las mejores

universidades del mundo; propicia un balance entre los conocimientos básicos que proporciona de Matemáticas, Física y Química; ha alcanzado un alto grado de madurez con reconocimiento pleno de la UNAM, al lograr que sus alumnos se constituyan en estudiantes de alta calidad y por su contribución para formar ingenieros capaces, competitivos, inquisitivos, con amor por el saber, orgullosos y plenamente comprometidos con la Universidad y con la sociedad, con elevadas metas y valores éticos.

Todo esto fruto de la calidad de su planta docente, estructurada, con estabilidad laboral, que además del dominio de sus áreas de conocimiento trabaja interdisciplinariamente con cabal conocimiento de su papel docente. Sus académicos poseen una gran fortaleza en valores humanos, están plenamente comprometidos y aplican todo el potencial tecnológico de frontera que la Facultad ha puesto a su alcance para su actualización continua y para diseñar y aplicar modelos didácticos novedosos con tecnologías de vanguardia, que estimulan el aprendizaje significativo de los alumnos, propiciando el trabajo en equipo y el autoaprendizaje; conforme la filosofía la División de Ciencias Básicas coadyuvan a la formación integral de ingenieros desde la apropiación y generación de conocimiento, hasta consolidar una comunidad académica reconocida, con visión universal y comprometida con el desarrollo nacional.

Es una División que continúa realizando esfuerzos tendientes a constituirse en propiciadora de evaluaciones continuas, de revisiones y, siempre que proceda, de actualizaciones; define indicadores que aportan información útil para el desarrollo de programas de mejoramiento de la calidad en los servicios que ofrece, de los procedimientos que emplea y de los recursos que posee, promoviendo una verdadera cultura ecológica y manteniendo convenios con el sector productivo para conseguir un beneficio mutuo que implica ingresos adicionales.

Los vínculos de colaboración de la DCB con el Bachillerato de la UNAM, para ayudar a los alumnos que ingresan a la Facultad, se han consolidado como resultado de la mejora continua y han sido ejemplo para otras entidades universitarias; los lazos con las otras Divisiones de la Facultad de Ingeniería permiten vigilar continuamente los contenidos de los programas de asignatura para que estén acordes a las necesidades del país; su colaboración con otras universidades nacionales e internacionales y dependencias universitarias promueve y estimula conjuntamente la investigación educativa y el desarrollo tecnológico, con la participación entusiasta de profesores y alumnos de la División.

Como resultado de la mejora de la calidad de vida en el trabajo, el personal de la DCB trabaja con gusto y entusiasmo, pues el ambiente que se respira es de camaradería y colaboración, se ha alcanzado una plena comunicación entre sus miembros y se han tomado las medidas necesarias para que el problema de la inseguridad en la DCB esté resuelto."

INFRAESTRUCTURA Y SERVICIOS DE CÓMPUTO

En la DCB existen dos redes locales: una que brinda servicio tanto a las coordinaciones de Matemáticas Básicas, Física Experimental y Química y de Ciencias Aplicadas, además de laboratorios de Electricidad y Magnetismo, Mecánica, Termodinámica, Química y Óptica, así como a un pequeño sector de equipos en el área de jefatura; la otra red local da el servicio a equipos en los cuatro talleres de cómputo dedicados a la docencia y a los salones de clases del edificio ala poniente.

Cuenta actualmente con aproximadamente 350 equipos de cómputo, la mitad de éstos con procesadores obsoletos (Celeron, Pentium II, Pentium III y anteriores) y la otra mitad con procesadores más actuales (Pentium IV, Pentium D, Core Duo, Core 2 Duo y equivalentes). También tiene en operación 6 servidores que asisten a la red de cómputo, por la cual tienen acceso a Internet alumnos, académicos y personal administrativo. Cuenta con aproximadamente 50 equipos de impresión, que van desde impresoras de matriz de puntos, hasta impresoras de grandes volúmenes a color. También cuenta con diversos equipos de cómputo, como cámaras digitales, proyectores, scanners, lectoras ópticas, pizarrones electrónicos, entre otros.

Se cuenta con una página de Internet (http://dcb.fi-c.unam.mx), que proporciona distinta información a la comunidad de la DCB como páginas de profesores, información académica, calendario escolar, horarios, información del personal, distintas publicaciones, mapas curriculares, memorias de eventos organizados por la División y hosting de páginas de diversos eventos organizados por la División.

Así mismo, en la página se tienen montadas aplicaciones orientadas tanto al personal académico como al administrativo, donde se realizan operaciones de administración académica.

En la Red Interna de la DCB, se tienen montados dos servidores de archivos donde personal autorizado coloca documentos de interés académico y administrativo.

Se cuenta con un servicio de FTP para usos diversos.

Existen diversas bases de datos utilizadas para fines académico-administrativos, la mayoría de ellas implementadas en MS Access (planificadas a migrar a SQL a futuro) y una en SQL.

Asimismo, se brinda el servicio de lectura de exámenes en lectora óptica, usualmente los exámenes llamados colegiados y finales, con el objetivo de agilizar la calificación de los mismos y así poder entregar las calificaciones oportunamente a los alumnos y poder planificar de mejor manera el calendario de clases.

Se realiza también, la detección de fallas en el cableado estructurado, cuando existe sospecha de que algún nodo no funciona de manera adecuada, se realiza un diagnóstico para ver si el problema es de fácil solución o es necesario cambiar el cableado estructurado.

En general se da servicio de asesorías en materia de computación, al personal académico y administrativos que así lo requiera. Además de mantenimiento preventivo y correctivo al equipo de cómputo

Se brinda servicio de red los alumnos en cuatro salas de cómputo dedicadas a los alumnos, también a 19 salones de clase.

Las cuatro salas destinadas para los alumnos, cada una con alrededor de 150 PC´s, donde el profesor puede impartir su clase enfocada a la utilización de herramientas y software que facilitará a los alumnos tener una mejor comprensión de los problemas planteados en la materia. También se promueve la interacción en la clase, ya que cada alumno cuenta con un equipo propio, donde puede seguir paso a paso, o resolver lo indicado por el profesor.

En los 19 salones de clases, los profesores tienen acceso a herramientas de cómputo (PC, proyector, pizarrón electrónico) para poder ofrecer una mejor calidad de cátedra y fomentar en sus alumnos una mayor y mejor comprensión de la materia que está impartiendo.

Para el personal académico, se cuenta con acceso a la red desde el Taller de Cómputo para Académicos, coordinaciones, departamentos, cubículos de profesores de carrera, jefatura y laboratorios.

Dicha red, provee la salida a Internet desde los equipos que la conforman y permiten el acceso a los diversos servicios que se ofrecen en la Red Local.

Una sala de cómputo (TCA), donde se los académicos tienen acceso a equipo de cómputo, servicios de impresión, asesoría, acceso a la lectora óptica, mantenimiento preventivo y correctivo de equipo.

La DCB cuenta con acceso a Internet y a la Red Local desde las distintas coordinaciones académicas (Matemáticas, Ciencias Aplicadas y Física y Química), los laboratorios (de Mecánica, Electricidad y Magnetismo, Termodinámica, Química y Física), y las áreas de jefatura.

Se cuenta con una red inalámbrica administrada por DGSCA (Red Inalámbrica Universitaria, RIU), que brinda servicio a toda la comunidad académica en los salones del primer y segundo pisos del edificio ala poniente del Anexo.

En total se cuenta con alrededor de 250 nodos repartidos entre las distintas coordinaciones, cubículos de profesores, laboratorios, salones de clases, jefatura y salas de cómputo tanto para profesores, como para alumnos. Administrados por personal de la División.

SITUACIÓN ACTUAL DE LA SEGURIDAD EN CÓMPUTO

Actualmente en la DCB, actualmente se cuenta con un esquema de seguridad no escrito, pero que sigue una serie de normas básicas para la seguridad de la información, como por ejemplo la colocación y configuración de firewalls que filtran el tráfico entrante y saliente de las redes locales, instalación de software antivirus, antispyware, removedor de software malicioso, reglamentos de uso de las áreas de cómputo y recomendaciones de seguimiento a las políticas de seguridad de la Facultad de Ingeniería emitidas en el año 2003, entre otras. Dicha documentación por lo general, no es seguida en su totalidad por los usuarios, ya sea por desconocimiento o por ignorancia.

Dicho esquema no es del todo completo, por lo que se han presentados diversos incidentes como:

- Utilización de protocolos P2P o Torrent
- Instalación de software malintencionado como spyware, troyanos, virus, etc… (lo que ha causado que un gran número de computadoras se hayan infectado, en algunos casos se pudo remover dicho software con herramientas antivirus o antispyware, pero en la mayoría se tuvo que formatear el equipo para removerlo completamente, lo que ha causado una disminución en la productividad de los usuarios)
- Malfuncionamiento o negación de servicios en la red local
- Equipo no actualizado correctamente
- Uso inadecuado por parte de los usuarios de los equipos
- Malfuncionamiento general del equipo
- A nivel de seguridad física se han presentado robos de equipo tanto en salones, como en cubículos de académicos, entre otros

No se cuenta con un documento escrito que indique un plan de contingencia, ni con un esquema de recuperación de información.

CAPÍTULO 1. ANTECEDENTES DE SEGURIDAD EN CÓMPUTO

En este capítulo abarcará desde distintos conceptos de seguridad informática, gestión de riesgos, ataques informáticos, tipos de controles y algunos ejemplos de mecanismos de seguridad.

1.1 SERVICIOS DE SEGURIDAD

Un servicio de seguridad es una característica que debe de tener un sistema

Al hablar de seguridad se tienen que definir los servicios en los que está basada. Son seis: confidencialidad, integridad, autenticación, disponibilidad, control de acceso y no repudio. Algunos autores sólo consideran los primeros tres y los llaman la *Triada de la Seguridad (CIA).*

- **Confidencialidad [1]**

Establece que la información sólo sea accesible desde entidades (dispositivos, procesos o usuarios) autorizadas. Existe la confidencialidad de datos y la confidencialidad de flujo, ambas se pueden obtener mediante *cifrado*.

La confidencialidad de datos es para el intercambio entre las entidades, ya sea toda la información, o sólo un segmento de ésta.

La confidencialidad de flujo protege la identidad de las entidades, tanto la de origen, como la destino.

- **Integridad [1]**

Asegura que la información no ha sido alterada o destruida de manera no autorizada. La alteración puede ser mediante escritura, cambio, borrado, creación o reenvío no autorizado. Existe la integridad de datos y la integridad de secuencia de datos.

[1] ISO 7498-2

La integridad de datos se puede conseguir por ejemplo mediante una función hash. La integridad de secuencia de datos se puede obtener mediante el uso de *time-stamps*.

- **Autenticación [2]**

Es la verificación de la identidad de un usuario, proceso o dispositivo, previo a permitir el acceso a un recurso. Existe la autenticación de origen, de destino, de contenido, de llaves y de transacciones.

Tanto la autenticación de origen como de destino, se aseguran de que ambas entidades en una comunicación sean válidas.

La autenticación de contenido asegura que la información sea legítima.

La autenticación de llaves asegura que ninguna entidad no autorizada ha tenido acceso a la llave privada en un cifrado asimétrico.

La autenticación de transacciones asegura que una transacción sea legítima, además de que los datos sean únicos y temporales. Se logra mediante protocolos criptográficos como SET (Secure Electronic Transaction).

Entendiéndose como identificación, puede basarse en:

- Algo que se sabe, por ejemplo una contraseña.
- Algo que se tiene, como un token.
- Algo que se es, por ejemplo el uso de biometría.

Lo más seguro es la utilización de dos o más factores de autenticación que pertenezcan a grupos distintos.

Existe la autenticación *directa* e *indirecta*. En la directa sólo intervienen en el proceso las partes interesadas, mientras en la indirecta se requiere la mediación de una tercera parte confiable que actúe como autoridad que avale a ambas.

[2] NIST IR-7298

La autenticación puede ser *unidireccional* o *mutua*, es decir, puede requerirse que sólo una parte o ambas se autentiquen.

- **Disponibilidad [1]**

Indica que la información puede ser accesible y utilizable por entidades autorizadas, en el momento que sea requerida. Este servicio es prácticamente imposible de garantizar en entornos donde se requiera el uso de redes públicas como Internet.

- **Control de Acceso [2]**

Es el otorgamiento de permisos o su revocación, para lograr acceder a un recurso. Usualmente se requiere que el sistema destino sea el que lleve dicho control protegiéndose así de usos no autorizados o manipulación.

Está muy ligado al servicio de autenticación. Incluso, usualmente los mecanismos que garantizan el control de acceso, también pueden llegar a garantizar la autenticación.

- **No Repudio [1]**

Establece que las entidades involucradas en una comunicación no puedan negar su participación. El no repudio de origen, protege al receptor de que el emisor niegue haber enviado la información. El no repudio de recepción protege al emisor de que el receptor niegue haber recibido la información. Para lograr el no repudio, se utilizan por ejemplo las firmas digitales.

No todos los servicios tienen que estar definidos al mismo tiempo, y la importancia de cada uno de ellos dependerá de la misión de la organización.

Existen mecanismos de seguridad que pueden otorgar un buen nivel asociado a cada servicio de seguridad. Cabe destacar que no es viable la implantación de mecanismos cuyo costo sea mayor al costo relativo de la información a proteger.

En la Tabla 1.2 se muestran las capas del modelo OSI en las que se puede llegar a garantizar los distintos servicios de seguridad.

Haciendo la similitud entre el modelo OSI, con el TCP/IP el resultado es muy similar, ya que cada capa tiene su análogo en el otro modelo, como se muestra en la Figura 1.1 y los mecanismos que pueden garantizar los servicios en este modelo se muestran en la Figura 1.3

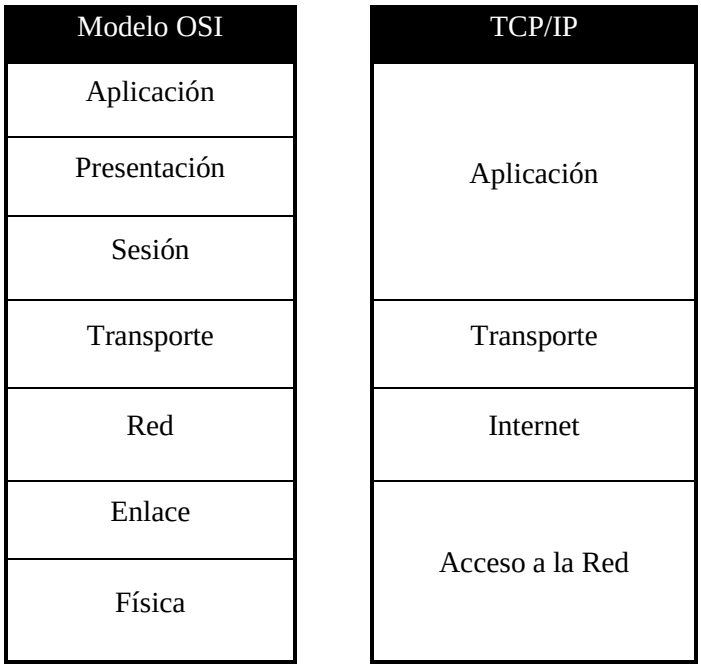


Figura 1.1 Modelos OSI y TCP/IP

SERVICIO DE SEGURIDAD	CAPA DEL MODELO OSI						
	Física 1	**Enlace 2**	**Red 3**	**Transporte 4**	**Sesión 5**	**Presentación 6**	**Aplicación 7**
CONFIDENCIALIDAD	Cifrado, control de ruteo y traffic padding	Cifrado y control de ruteo	Cifrado, control de ruteo y traffic padding	Cifrado y control de ruteo			Cifrado, control de ruteo y traffic padding
INTEGRIDAD			Cifrado, verif. de integridad y firma digital	Cifrado, verif. de integridad y firma digital			Cifrado, verif. de integridad y firma digital
DISPONIBILIDAD							
AUTENTICACIÓN			Cifrado, firma digital y mecanismos de autenticación	Cifrado, firma digital y mecanismos de autenticación			Cifrado, firma digital y mecanismos de autenticación
CONTROL DE ACCESO			Mecanismos de control de acceso	Mecanismos de control de acceso			Mecanismos de control de acceso
NO REPUDIO							Firma digital, verif. de integridad

Tabla 1.2 Servicios de seguridad y modelo OSI

SERVICIO DE SEGURIDAD	CAPA DEL MODELO TCP/IP			
	Acceso a la Red	**Internet**	**Transporte**	**Aplicación**
CONFIDENCIALIDAD	Cifrado, control de ruteo y traffic padding	Cifrado, control de ruteo y traffic padding	Cifrado y control de ruteo	Cifrado, control de ruteo y traffic padding
INTEGRIDAD		Cifrado, verif. de integridad y firma digital	Cifrado, verif. de integridad y firma digital	Cifrado, verif. de integridad y firma digital
DISPONIBILIDAD				
AUTENTICACIÓN		Cifrado, firma digital y mecanismos de autenticación	Cifrado, firma digital y mecanismos de autenticación	Cifrado, firma digital y mecanismos de autenticación
CONTROL DE ACCESO		Mecanismos de control de acceso	Mecanismos de control de acceso	Mecanismos de control de acceso
NO REPUDIO				Firma digital, verif. de integridad y notarización

Tabla 1.3 Servicios de seguridad y TCP/IP

1.2 AMENAZA, VULNERABILIDAD Y RIESGO

- **Amenaza [3]**

Una amenaza es cualquier circunstancia o evento con el potencial de impactar desfavorablemente las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), recursos de la organización, o individuos a través de un sistema de información vía acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicios.

Las amenazas pueden clasificarse de acuerdo a su origen en: naturales, humanas y ambientales.

Entonces, si no se tiene muy claro qué podría constituir una amenaza a un sistema de TI, se deberá de hacer la pregunta: ¿qué puede suceder?

Existen principalmente cuatro tipos de contingencias principales que alteran el usual comportamiento de una comunicación entre dos entidades (personas, procesos o dispositivos) a través de un canal: interrupción, intercepción, modificación y fabricación.

- Interrupción: Es cuando no se concreta la comunicación, por lo que se afecta la disponibilidad de un recurso. Por ejemplo, el apagado de un servidor que requiere alta disponibilidad.
- Intercepción: Se da cuando una entidad no autorizada logra obtener acceso a la comunicación. Afecta la confidencialidad. Por ejemplo, la intervención del canal de comunicación para obtener contraseñas.
- Modificación: En el caso de que una entidad no autorizada logra tener acceso a la comunicación y la altera para luego enviársela a la entidad destino original. Afecta la integridad. Por ejemplo, alterar los registros de una base de datos
- Fabricación: Es cuando la entidad no autorizada crea objetos falsificados en un sistema, pretendiendo ser una entidad autorizada. Afecta la autenticación y está relacionada con el no repudio. Por ejemplo, la suplantación de la entidad origen.

[3] NIST SP 800-30

- **Vulnerabilidad [3]**

Es una debilidad o falla de un sistema de información, diseño, procedimientos de seguridad, controles internos, o ejecución que puede ser explotada o desencadenada por una fuente de amenaza, causando una violación de seguridad o un incumplimiento de las políticas de seguridad del sistema.

- **Riesgo [3]**

Riesgo es una medida de la probabilidad de que una amenaza, a través de una vulnerabilidad, afecte el correcto funcionamiento de un sistema; tomando en cuenta el impacto resultante de dicho evento en una organización.

Entonces, el riesgo es una función de la probabilidad, de que una fuente de amenaza, altere el correcto funcionamiento de un sistema, a través de una vulnerabilidad, tomando en cuenta el potencial impacto resultante en la organización. Ver figura 1.4

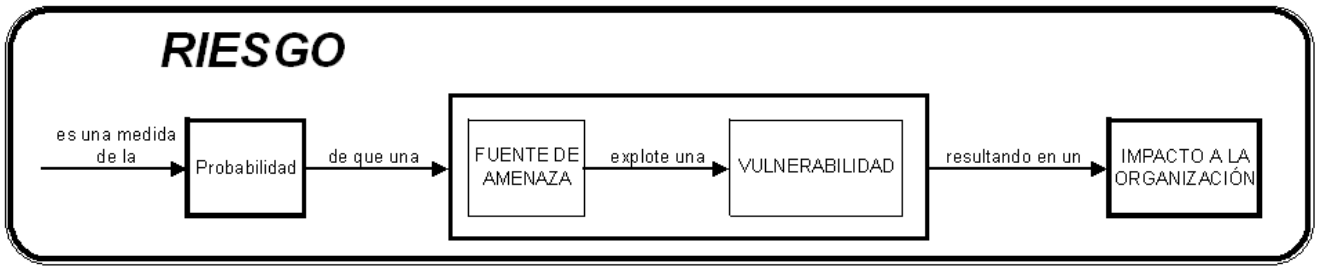


Figura 1.4 Concepto de Riesgo

1.3 GESTIÓN DE RIESGOS

Es de utilidad para la identificación de los puntos más débiles en un sistema de TI. Como resultado de este proceso se tienen los controles de seguridad más adecuados de acuerdo a su viabilidad y costo. También indica qué áreas tienen que contar con un Plan de Recuperación de Desastres (DRP) y un Plan de Continuidad de Negocio (BCP). Además de que permite la realización de políticas de seguridad que vayan de acuerdo con la misión de la organización.

Existen dos enfoques de gestión de riesgos: cuantitativo y cualitativo.

- *Cuantitativo*. Busca obtener valores numéricos, casi siempre de carácter económico, de los activos que se están estudiando y su pérdida posible. Los resultados obtenidos son expresados de igual manera en porcentajes, probabilidades de ocurrencia, pesos, entre otros. Al momento de mostrar los resultados a las altas esferas de las instituciones, es más sencillo ya que está expresado en términos económicos. Los cálculos son muy complejos. Es muy ardua la recolección de información en etapas iniciales. Es demasiado complicado llevarse a cabo, debido a que es muy difícil asignársele valores monetarios a la información, es decir, para contestarse por ejemplo cuánto puede valer mi información, un registro en mi base de datos, mis archivos de configuración, etc., en muchas ocasiones ni siquiera los altos mandos lo tienen claro. Sólo es sencilla la asignación de valores monetarios a los activos físicos, por su precio en el mercado por ejemplo.
- *Cualitativo*. No se requiere la asignación de valores numéricos a los activos que se encuentren en estudio. Los resultados son subjetivos, pero son basados en las interpretaciones y experiencia de los dueños de la información, ya que ellos tienen muy en claro qué tan crítica o sensible es. Los cálculos son sencillos. La calidad de estos estudios dependerá de la objetividad con que se lleve a cabo el proceso de recopilación de información.

Hay que aclarar que la *gestión de riesgos* es un proceso que muestra el estado de la seguridad al momento de la realización del estudio, ya que un sistema de TI no es estático, es decir, cambian los activos, se identifican nuevas vulnerabilidades y amenazas, motivaciones, etc. por lo que habrá que realizar un nuevo estudio cada cierto tiempo o en el caso de un cambio radical en las tecnologías utilizadas.

La Gestión de Riesgos abarca tres procesos: el *Análisis de Riesgos*, la *Mitigación de Riesgos* y el proceso de *Gestión y Evaluación*.

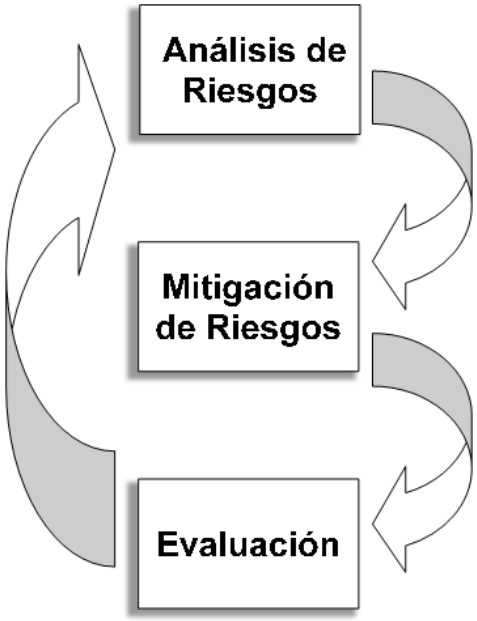


Figura 1.5 Esquema de Gestión de Riesgos

1.3.1 ANÁLISIS DE RIESGOS

También llamado *Evaluación de Riesgos*, es el proceso de identificar los riesgos de operación (incluyendo misión, visión, funciones, imagen o reputación), y los recursos de una organización o de un individuo, mediante la determinación de distintos parámetros como:

- Probabilidad de ocurrencia.
- Impacto resultante.
- Controles de seguridad que mitiguen el impacto.

Durante la *evaluación de riesgos*, se realizan los análisis de amenazas (donde se identifican las fuentes de amenaza potenciales y sus causas) y de vulnerabilidades (mediante el cual se identifican las vulnerabilidades a las que está expuesto el sistema y las acciones que podrían ocasionarse si se llegan a explotar).

1.3.2 MITIGACIÓN DE RIESGOS

Es el proceso mediante el cual los riesgos identificados en la evaluación de riesgos son abordados, buscando una disminución en el impacto potencial en la organización. Incluye un

estudio de costo-beneficio, selección y evaluación de controles de seguridad y asignación de responsabilidades. Es, en sí, una estrategia que busca atenuar los riesgos.

1.3.3 GESTIÓN Y EVALUACIÓN

En el tercer proceso se considera que los sistemas o las redes de una organización están en continua expansión, por lo que pueden llegar a cambiar sus componentes, el software utilizado, el personal, entre otras cosas. Por lo que surgirán nuevos riesgos, o algunos previamente mitigados podrán volver a ser una preocupación, o incluso podrían desaparecer.

Se deberá de indicar la periodicidad con la que se tendrá que llevar a cabo la *gestión de riesgos*. Dicho proceso no deberá de realizarse sólo porque es requerido por leyes (en las Agencias Federales de los EU, es obligatorio llevarla a cabo cada 3 años), sino porque es una buena práctica que apoya los objetivos de una organización. El tiempo entre la ejecución de la gestión, tendrá que ser lo suficientemente flexible para permitir cambios cuando éstos sean justificados, como algún cambio mayor en la tecnología de TI utilizada o en el ambiente de la organización, debido a cambios en sus políticas.

Algunos autores como David Nicol, de la Universidad de Illinois, agregan un último proceso definido como *Comunicación de Riesgos*, que consiste en la presentación de lo obtenido durante los dos procesos anteriores de una manera fácilmente entendible al personal que toma las decisiones y/o al público.

Una Gestión de Riesgos efectiva, deberá de tener el compromiso de los directivos, el completo apoyo y participación del personal a cargo de los sistemas, la cooperación y concientización de los usuarios, que deberán de seguir procedimientos y cumplir con los controles implantados y una evaluación continua.

Existen distintas metodologías para la *gestión de riesgos*, por ejemplo la propuesta en el NIST SP 800-30 (más adelante explicada a detalle), OCTAVE, Magerit, ISO 27005, entre otras, que brevemente serán explicadas a continuación.

- **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation). Desarrollado por el Sofware Engineering Institute de la Universidad de Carnegie Mellon. Es una metodología de planeación y evaluación basada en riesgos. Se dice que es auto-dirigida,

es decir, las personas dentro de la organización donde se aplica asumen la responsabilidad de establecer la estrategia de seguridad organizacional.

Maneja dos aspectos fundamentales, la seguridad operacional y prácticas de seguridad. Cuando OCTAVE es aplicado, las organizaciones realizan las decisiones de protección de información basándose en los riesgos que afectan la confidencialidad, integridad y disponibilidad de los recursos relacionados con los recursos que la afectan.

Todos los factores involucrados con los riesgos son tomados en cuenta para los procesos de toma de decisiones, permitiendo a la organización hacer coincidir una estrategia con los riesgos de seguridad existentes.

Se debe de conformar un equipo de análisis en la organización, que realice las siguientes actividades:

-Identificación de los recursos importantes
-Enfocar las actividades de análisis de riesgos en aquellos que se han identificado como críticos
-Considerar la relación entre los recursos críticos y sus amenazas y vulnerabilidades
-Evaluar los riesgos en un contexto operacional
-Creación de una estrategia de protección basada en prácticas, así como planes de mitigación para reducir los riesgos en los recursos críticos de la organización

La metodología OCTAVE, consta de tres fases:
- *Fase 1*. Construcción de perfiles de amenazas, basados en los recursos: Se determina qué es importante para la organización y qué se está haciendo para proteger dichos recursos. Luego se seleccionan los críticos y se describen sus requerimientos de seguridad. Finalmente, se identifican sus amenazas, creando un perfil de amenaza para cada recurso crítico.

- *Fase 2*. Identificación de las vulnerabilidades en la infraestructura: Se realiza una evaluación de la infraestructura de la información. Se analizan las rutas de acceso a la red, se identifican los tipos de componentes de tecnología de la información relacionados a los recursos críticos. Luego, se determina el alcance en que cada tipo de componente es resistente a ataques sobre la red.

- Fase 3. Desarrollo y Planeación de la Estrategia de Seguridad: Se identifican los riesgos en los recursos críticos y se deciden las acciones a tomar con éstos. Se realiza una estrategia de protección para la organización y planes de mitigación, basados en la información recopilada anteriormente.

Figura 1.6 OCTAVE

Los elementos o requerimientos esenciales del enfoque OCTAVE son agrupados en un conjunto de criterios. Se han desarrollado en la actualidad dos conjuntos de criterios: el método OCTAVE, diseñado para grandes organizaciones; y el método OCTAVE-S para organizaciones pequeñas, aunque se encuentra aún en desarrollo.

- La metodología **Magerit** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), desarrollada en Madrid. Se enfoca en el desarrollo de un Proyecto de Análisis y Gestión de Riesgos, que consta de tres grandes pasos: planificación, análisis y gestión; cada uno consta de distintas actividades que están estructuradas por distintas tareas.

  Se indica que hay que establecer un comité de dirección, un comité de seguimiento, grupos de interlocutores, un promotor, un director del proyecto y un enlace operacional.

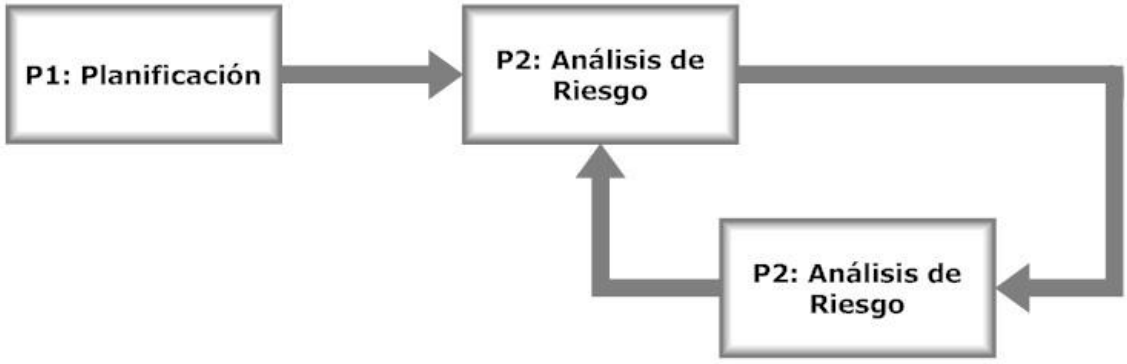


Figura 1.7 Magerit

Los tres procesos constan de lo siguiente:

- *Proceso 1*: Planificación. Se establecen las consideraciones previas al proyecto necesarias, se investiga la oportunidad de su realización, se definen los objetivos y el alcance, se apartan los recursos tanto materiales, como humanos y se procede a la inicialización del proyecto.
- *Proceso 2*: Análisis de Riesgos. Es en donde se identifican los activos, su valor y relación entre ellos, las amenazas significativas, los mecanismos de seguridad, y se estima el impacto y el riesgo.
- *Proceso 3*: Gestión de Riesgos. En este proceso, se realiza la elección de una estrategia de mitigación de riesgos, se determinan los mecanismos, se diseña y lleva a cabo el plan de seguridad.

Es una metodología de gestión de riesgos cuantitativa, por lo que se debe de tener muy bien en cuenta el valor de los activos informáticos que podrían resultar un riesgo para la organización.

- **ISO 27005**, publicado en julio del 2008, En dicho estándar no se define si deberá de realizarse un estudio cualitativo o cuantitativo. Ha sido diseñado para el estudio de los riesgos a través de un Sistema de Gestión de la Seguridad Informática (SGSI) SGSI, es decir, está enfocado a la obtención de la certificación ISO 27001.

La siguiente figura muestra los pasos que esta metodología:

Figura 1.8 ISO 27005

1.4 ANATOMÍA DE UN ATAQUE

Un ataque es el acto de intentar evitar los controles de seguridad de un sistema. Un ataque puede ser activo o pasivo. Un ataque activo tiene como resultado la modificación de datos, mientras que uno pasivo tiene como consecuencia la divulgación de información. No necesariamente tiene que ser exitoso, es decir, se puede lanzar un ataque sin obtener los resultados deseados, éstos dependerán de qué tan vulnerable es el sistema objetivo y la efectividad de las medidas para mitigar los ataques con las que cuenta.

No existe una metodología establecida para el lanzamiento de un ataque a través de la red. Sin embargo, existen ciertas prácticas que son comunes a la mayoría de éstos:

Figura 1.9 Anatomía de un Ataque

- **Descubrimiento**. Consiste en la identificación del(os) objetivo(s) a atacar.

Se puede realizar una recopilación de información que se encuentra pública a cualquier usuario de Internet, que se refiera al sitio u organización objetivo.

Por ejemplo, puede utilizarse el motor de búsqueda de Google, que brinda una amplia gama de información utilizando una técnica llamada Google Hacking, que consiste en la realización de consultas complejas utilizando los operadores con que Google cuenta (por ejemplo, inurl:, intitle:, filetype:, site:, etc), incluso existe software que el mismo Google ofrece para realizar este tipo de búsquedas avanzadas por medio de las cuales se pueden obtener listados de servidores vulnerables, mensajes de error que revelan demasiada información, archivos con información sensible, archivos que contienen passwords, nombres de usuarios, páginas de login de acceso a servicios, bitácoras de firewalls, bitácoras de honeypots, información de redes, bitácoras de IDS´s, sitios que contienen directorios de archivos con información que no debería de ser divulgada, información relacionada a ventas por internet, diversos dispositivos online, detección de servidores de web, direcciones IP, correos electrónicos, entre muchas otras cosas.

También pueden hacerse uso de las diversas bases de datos disponibles en la red, por ejemplo la base de datos *Whois*, que permite obtener información de direcciones IP, DNS´s, correos electrónicos, números telefónicos, nombres de administradores o domicilios.

Una de las técnicas más recurridas es el empleo de la ingeniería social en esta fase, ya que muchas veces la forma más fácil de obtener información es simplemente preguntándola.

Al finalizar el descubrimiento se tendrá una lista de información que podría ser de utilidad en fases posteriores, como por ejemplo los equipos que están expuestos en la red (web, smtp, dns, etc), inclusive se podría contar en este momento con datos como las subredes existentes en una organización.

- **Enumeración**. Se trata de un reconocimiento inicial.

En esta etapa el atacante realiza un inventario de la red objetivo, incluyendo un barrido de puertos (para tener una idea de cuáles se encuentran cerrados, abiertos o filtrados) y/o la identificación de banners de servicios (para así saber qué servicios tiene activos y la versión de éstos), identificación del sistema operativo del servidor.

Usualmente se utiliza la herramienta nmap (la cual se explicará a detalle más adelante), considerada la "navaja suiza para escaneo de redes", puede utilizarse, por ejemplo con los siguientes parámetros (aunque el escaneo es muy escandaloso, es decir, se registra en los logs del servidor objetivo, pero sirve para ejemplificación):

nmap –v –sTUV –P0 –p- IP_Objetivo

Puede obtenerse información valiosa, como por ejemplo:

Puerto 22/TCP abierto, OpenSSH 2.1.1

Puerto 53/TCP abierto, Bind 9.4.1

Puerto 80/TCP abierto, Apache 2.2.4

También pueden utilizarse otras herramientas de escaneo de redes, actualmente existe una gran variedad, ya sean libres o propietarios, pero la herramienta estándar de facto es nmap.

- **Mapeo de Vulnerabilidades**. En esta fase, se identifican las vulnerabilidades que pueden llegar a afectar al objetivo.

Puede realizarse tanto de manera manual, como automática.

El mapeo de vulnerabilidades manual, se puede llevar a cabo haciendo búsquedas de las aplicaciones detectadas previamente con las vulnerabilidades publicadas.

La manera automática aprovecha la gran cantidad de programas llamados Vulnerability Scanners, que cuentan con bases de datos de aplicaciones/vulnerabilidades, y logran identificar la mayoría de las vulnerabilidades a las que está expuesto determinado sistema. Sin embargo, muchas veces dichos programas arrojan "falsos positivos" (cuando se indica que un sistema es propenso a cierta vulnerabilidad, cuando no ocurre esto en realidad), el administrador (o en este caso el atacante) deberá de saber cuándo se encuentra con un falso positivo, o cuando se encuentra de verdad una vulnerabilidad que pueda ser explotada.

Algunos scanners de vulnerabilidades disponibles son:

- **Nessus**. Es el scanner de vulnerabilidades más utilizado, hasta el 2008 era software libre, actualmente existe una licencia para usuarios caseros, que es un poco limitada pero sirve para los propósitos en esta fase de un ataque. Es el mejor scanner de vulnerabilidades para UNIX. Se encuentra en constantes actualizaciones y cuenta con más de 20000 plugins. Puede realizar revisiones de autenticación tanto remotas como locales, cuenta con un lenguaje de scripts nativo para escribir plugins propios o entender mejor los existentes. Trabaja en una arquitectura cliente-servidor.
- **GFI LanGuard.** Esta herramienta primero escanea redes para detectar qué equipos se encuentran activos, luego trata de detectar qué sistema operativo está corriendo; en equipos Windows también identifica qué service pack tiene instalado, parches de seguridad faltantes, access points inalámbricos, dispositivos USB conectados, archivos compartidos, puertos abiertos, servicios/aplicaciones instalados, llaves de registros claves, passwords débiles, usuarios, grupos, entre otras cosas.
- **MBSA.** Microsoft Baseline Security Analyzer. Esta herramienta, aunque es de Microsoft, puede descargarse de manera gratuita de la red. Trabaja en conjunto con el agente de windows update y su infraestructura.

Otros scanners de vulnerabilidades disponibles son: Retina, Core Impact, ISS Internet Scanner, X-Scan, Sara, QualysGuard, SAINT, entre otros.

También existen los llamados scanners de web (Web Vulnerability Scanners), que permiten auditar (o en el caso de los atacantes identificar) las vulnerabilidades a las que está expuesto su sitio web, que son los equipos que se encuentran más expuestos generalmente, y por medio de los cuales se puede lograr saltar firewalls. Algunos de los más populares son: Nikto, Paros Proxy, WebScarab, Whisker, Wikto, Acunetix WVS, entre otros.

En la mayoría de las ocasiones, el atacante intentará primero con las vulnerabilidades que no sean tan complicadas de explotar, y si con éstas no logra tener éxito tratará con las demás.

Puede obtenerse por ejemplo como resultado:

Apache Web Server Multiple Module Local Buffer Overflow Vulnerability (http://www.securityfocus.com/bid/8911) para la versión de Apache 2.2.4

- **Actividades de Penetración**. En esta etapa es cuando se lleva a cabo el ataque.

El ataque deberá de ser lo más rápido posible, para así tener mayores posibilidades de evitar ser detectado, también se busca que no sea auditable por lo que no deberá de dejar rastros, como por ejemplo líneas en bitácoras o cambios muy llamativos en el sistema (a menos que ese sea el objetivo del ataque).

Pueden utilizarse exploits disponibles en sitios de Internet como packetstormsecurity o securityfocus que ofrecen una serie de herramientas y archivos con líneas de código para explotar vulnerabilidades publicadas. Sin embargo, siempre se deberá de revisar el código para entender qué se está realizando, también para tener la certeza de que no se está ejecutando código que potencialmente pueda dañar nuestro equipo.

Pueden realizarse ataques a los mecanismos de autenticación, tanto en línea como fuera de línea, o ataques que se basan en fallas de configuración de los servidores.

Pueden realizarse ataques de cualquier índole como por ejemplo, buffer overflows, inyección de código, código malicioso, DoS, entre muchos otros, algunos de los cuales serán explicados posteriormente.

Sólo la imaginación del atacante es el límite de lo que se pueda realizar, mientras la información, la tecnología y los controles de seguridad establecidos lo permitan.

- **Consolidación**. Son las actividades realizadas después de lograr penetrar en el sistema.

Una vez penetrado el sistema, el atacante buscará escalar los privilegios con los que logró ingresar. Una vez que se tienen los privilegios de administrador en Windows, o de root en UNIX se puede recopilar toda la información importante del sistema o información sensible de los usuarios.

En la mayoría de las ocasiones, se buscará garantizar el acceso a un sistema para ocasiones futuras mediante caballos de troya, puertas traseras, ingreso de usuarios nuevos, suplantación, etc.

Frecuentemente los atacantes intentan penetrar distintos sistemas, para así poder lanzar ataques a otros objetivos y así buscar evitar ser rastreados.

1.4 EJEMPLOS DE ATAQUES

- **Mapeo de Redes**

El mapeo de redes es una técnica, que en sí misma no constituye un ataque, sin embargo usualmente lo antecede para poder obtener información valiosa del objetivo y así identificar las vulnerabilidades que se pueden explotar y el reconocimiento del camino más fácil para poder penetrar en el sistema.

La herramienta más utilizada es nmap, que es una utilidad gratuita y con licencia de código abierto escrita por el hacker Gordon Lyon, mejor conocido en Internet como *Fyodor*. Sirve para una gran variedad de casos, como realizar inventarios de redes, escaneo de puertos TCP y UDP, identificación de versiones de programas utilizados para brindar servicios, detección de Sistema Operativo, etc. Es portable, ya que se puede correr desde casi cualquier Sistema Operativo (Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS-X, HP-UX, entre otros).

Su utilización es la siguiente:

#nmap [Tipo de Escaneo(s)] [Opciones] {objetivo}

El objetivo puede indicarse en forma de hostname, dirección IP, segmentos de red, una lista o hosts aleatorios, también pueden excluirse objetivos.

A menos que se le indique, para casi la mayoría de los casos, nmap primero realiza el descubrimiento de hosts, y después realiza el escaneo de puertos. El descubrimiento de hosts va más allá de un simple ping ICMP. Si no se ingresa ningún parámetro, nmap envía un paquete TCP ACK hacia el puerto 80 y un ICMP echo request, si se es un usuario sin privilegios, envía un paquete TCP SYN, con la llamada al sistema connect( ), en lugar del ACK. A continuación se describen las opciones disponibles para el descubrimiento de hosts:

- List Scan (-sL)

Únicamente se obtienen los nombres canónicos de la IP o viceversa.

- Ping Scan (-sP)

Con ésta opción, se envía un paquete ICMP echo request y uno TCP ACK al puerto 80. Sirve para identificar si un host se encuentra activo o no.

- No Ping (-P0)

Se elimina la opción por default de intentar averiguar si el host objetivo está activo, por lo que si por ejemplo, se indica que se realice el escaneo a una red con direcciones privadas 192.168.10.0/24, se hará el envío a todos los 65535 hosts con los que cuenta la red.

- TCP SYN Ping (-PS)

Se envía un paquete TCP vacío al puerto 80, con la bandera SYN activada, por lo que el host objetivo supone que se quiere iniciar una conexión. Si se obtiene como respuesta un paquete RST, entonces el puerto se encuentra cerrado. Si se obtiene un paquete SYN/ACK, entonces el puerto está abierto, entonces la máquina que está ejecutando nmap envía un paquete RST para que no se establezca la conexión. Si el intento de conexión se cuelga hasta que se alcanza el tiempo de timeout establecido, nmap infiere que el host objetivo no está activo. nmap no toma en cuenta si el puerto está abierto o cerrado. Dependiendo de la respuesta sabrá si el host está activo o no.

- TCP ACK Ping (-PA)

Similar al TCP SYN Ping, solo que en lugar de enviar un paquete con la bandera SYN activada, se manda uno con la bandera ACK

- UDP Ping (-PU)

Envía paquetes UDP vacíos a los puertos seleccionados. El puerto por default que se utiliza es el 31338. Si se encuentra un puerto cerrado, el host responderá con un paquete ICMP de error que indica puerto inalcanzable, lo que indica que el host está activo. Si se prueba en un puerto que esté abierto, la mayoría de los servicios sólo ignorarán el paquete y no envía ninguna respuesta de vuelta, es por ésta razón que se utiliza el puerto 31338 que es demasiado improbable que esté en uso. Este tipo de escaneo es de utilidad para sortear firewalls que sólo filtren tráfico con protocolo TCP.

- ICMP Ping (-PE; -PP; -PM)

nmap puede utilizar los paquetes estándar ICMP que utiliza el paquete ping. Con la opción –PE se envía un paquete ICMP tipo 8 (echo request) al host, esperando como respuesta un tipo 0 (echo reply), para equipos activos, en otro caso el host no está activo. También se pueden hacer uso de los paquetes de tipo 13 (timestamp request) y tipo 17 (address mask request), esperando paquetes de tipo 14 (timestamp reply) y de tipo 18 (address mask reply), para verificar si un host está activo o no.

- ARP Ping (-PR)

Utiliza algoritmos optimizados que se encargarán de las peticiones ARP. Si se obtiene una respuesta, ni siquiera se tiene que tomar en cuenta los paquetes IP, porque ya se sabe que el host está activo. Esto hace que el escaneo ARP Ping sea más confiable que cualquiera que utilice protocolos TCP o UDP. Por lo que ésta es la opción por default de nmap cuando éste detecta que el objetivo está en una red local ethernet. Si no se requiere el ARP Ping en una red local, se deberá de indicar la opción: --send-ip.

- Traceroute (--traceroute)

El trazado de rutas es realizado por nmap después de que ha terminado el escaneo, con los resultados de esté para determinar el protocolo y puerto más probable por los que se alcanzará al objetivo. Trabaja con todos los tipos de escaneo, a excepción de Connect Scan y el Idle Scan.

- No DNS Resolution (-n)

Indica a nmap que nunca se realice la resolución inversa de DNS en las direcciones IP activas que encuentre.

- DNS Resolution for all targets (-R)

Lo opuesto a la opción –n, indica que siempre se haga la resolución inversa de las IP´s objetivo encontradas activas.

Para el escaneo de puertos, ofrece distintas técnicas:

- TCP SYN Scan (-sS)

Es la opción por default, realiza el escaneo a miles de puertos por segundo en redes rápidas que no tengan filtros como un firewall. También se conoce como Stealth Scan o Half-Open Scan, ya que se comporta de manera sigilosa ya que nunca se completa el three-way-handshake la que realiza una conexión TCP.

- TCP Connect Scan (-sT)

Es la opción cuando no se tienen los suficientes privilegios para poder mandar paquetes SYN, o se deseé escanear hosts IPv6. Utiliza la llamada al sistema connect( ), que lleva a cabo completa la conexión cuando se encuentra un puerto abierto, por lo que en el host objetivo se crea una bitácora de cada conexión establecida.

- UDP Scan (-sU)

Aunque la mayoría de los servicios más populares en Internet son protocolos TCP, existen algunos protocolos UDP muy importantes, como DNS, SNMP y DHCP. El escaneo UDP es

más lento y más difícil que el escaneo TCP. Envía un encabezado UDP vacío a cada puerto objetivo, si se obtiene de regreso un paquete de error ICMP de puerto inalcanzable (tipo 3, código 3), entonces el puerto se encuentra cerrado, cualquier otro error (tipo 3, códigos 1, 2, 9, 10 ó 13), indican que el puerto está siendo filtrado, si se obtiene como respuesta un paquete UDP, el puerto se toma como abierto. Este tipo de escaneo usualmente es lento debido a que la mayoría de los hosts en Internet regulan el número de mensajes de error ICMP por default, por ejemplo los Linux con kernel 2.4.20 los limita a un mensaje por segundo, por lo que un escaneo de 65535 puertos UDP llevará algo más de 18 horas. Puede ser combinado con algún tipo de escaneo TCP para escanear puertos de ambos protocolos.

- TCP NULL, FIN y XMAS (-sN; -sF; -sX)

Con el Null Scan, se envían paquetes TCP vacíos, sin ninguna bandera activada; con el FIN Scan se envían paquetes con la bandera FIN activada únicamente y con el XMAS Scan se envían paquetes con las banderas FIN, PSH y URG activadas. Se obtendrá un paquete RST si el puerto está cerrado y ninguna respuesta en caso de que esté abierto o filtrado. Se considera filtrado si se tiene como respuesta un mensaje de error ICMP. Estos tipos de escaneo, no funcionan con equipos con sistema operativo Windows o cierto tipo de equipo CISCO, puesto que no siguen el RFC 793, por lo que envían un paquete RST estando el puerto abierto o no.

- TCP ACK Scan (-sA)

Este tipo de escaneo no es utilizado para encontrar si un puerto se encuentra abierto, en cambio, es usado para determinar reglas de filtrado de firewalls y advertir el tipo de firewall existente (filtrado de paquetes o inspección de estado). Envía un paquete con la bandera ACK activada.

Cuando se escanean sistemas sin firewall, los puertos (abiertos o cerrados) devuelven un paquete TCP RST y nmap los marca como puertos sin filtrado. Los puertos que no responden o devuelven un paquete de error ICMP, son marcados como filtrados.

- TCP Window Scan (-sW)

Es idéntico al escaneo TCP ACK, que puede diferenciar puertos abiertos de cerrados, en lugar de sólo marcar puertos sin filtrado. Esto lo hace analizando el campo de *window* en el paquete RST devuelto, esto es, en algunos equipos, los puertos abiertos tienen un valor positivo en

dicho campo, mientras que los cerrados tienen un valor de cero. Sin embargo este tipo de escaneo no es siempre confiable, ya que explota un detalle de implementación de una minoría de sistemas y los sistemas que no la tengan, devolverán todos los puertos como cerrados.

- TCP Maimon Scan (-sM)

Utiliza una técnica descrita por Uriel Maimon, publicada en la revista Phrack #49 (Noviembre de 1996). Es muy similar a los escaneos NULL, FIN y XMAS, sólo que se envían paquetes con las banderas FIN y ACK activadas. De acuerdo al RFC 793, un paquete RST debe ser generado en respuesta a un paquete FIN/ACK, sin importar si está abierto o cerrado. Sin embargo, en muchos sistemas derivados de BSD simplemente desechan el paquete si el puerto está abierto, por lo que puede ser utilizado para diferenciarlos.

- Custom TCP Scan (--scanflags)

Con esta opción se pueden realizar escaneos diseñados por el usuario de nmap, activando las banderas TCP a su gusto. Se puede utilizar cualquier combinación con las banderas URG, ACK, PSH, RST, SYN y FIN.

Por lo que se podrá evitar ser descubierto por un IDS que ha agregado reglas específicas para los distintos tipos de escaneo con los que cuenta nmap.

- Idle Scan (-sI)

Utilizando esta opción, se puede escanear un objetivo sin siquiera haber mandado un solo paquete desde la IP donde se lanza el escaneo. Por lo que los IDS detectarán que el escaneo se realiza desde la máquina zombie. Lo que convierte a este tipo de escaneo en uno muy silencioso desde el punto de vista del que lo realiza. También permite conocer las relaciones de confianza entre distintas IP´s.

Básicamente consiste en tres pasos que se repiten para cada puerto:

1. Se obtiene el IPID (cada paquete en Internet cuenta con un número de identificación del fragmento, como la mayoría de los sistemas operativos sólo incrementan este número por cada paquete enviado, se puede saber cuántos paquetes se han enviado desde la última vez que se pidió por este IPID) de la máquina zombie.

2. Falsificar un paquete SYN desde la máquina zombie hacia el objetivo. Dependiendo del estado en que se encuentre el puerto, lo devuelto por el objetivo puede o no causar que su IPID sea incrementado.
3. Obtener el IPID del zombie de nuevo. El estado del puerto se determina comparando el valor del IPID con el que se tenía del paso 1. Un incremento de uno indica que el zombie no ha enviado ningún paquete exceptuando el de respuesta a la petición de su IPID, por lo que se sabe que el puerto está cerrado. Un incremento de dos indica que envió un paquete extra en respuesta a lo devuelto por el host objetivo, por lo que se sabe que el puerto está abierto. En caso de encontrar incrementos mayores a dos, significa que la máquina que se está utilizando como zombie no es apta para tal tarea

Con este tipo de escaneo no se puede diferenciar los puertos cerrados de los filtrados

- IP Protocol Scan (-so)

Mediante esta opción, se puede determinar qué protocolos (TCP, UDP, ICMP, IGMP, etc.) son soportados por el objetivo. Se envía paquetes IP, cambiando el valor del campo de 8 bits del protocolo. Lo que se busca es la devolución de mensajes de protocolo inalcanzable ICMP (tipo 3, código 2), lo que indicará que el protocolo está abierto, cualquier mensaje con un código distinto indicará que el protocolo está filtrado.

- FTP Bounce Scan (-b)

Se puede utilizar FTP para escanear los puertos de otro equipo indicando a un servidor FTP que envíe un archivo a los puertos que interesan de la máquina objetivo. El mensaje de error devuelto indicará el estado del puerto. Con este método se pueden evitar firewalls, ya que si se logra establecer una conexión con un servidor ftp vulnerable que se encuentre detrás de un firewall y escanear por puertos abiertos, esto es, si se logra leer y escribir en un directorio, se considerará el puerto como abierto. Sin embargo la mayoría de los servidores FTP vulnerables ya han sido parchados debidamente, pero aún siguen en Internet algunos que lo permiten.

Para la identificación de sistemas operativos (*OS fingerprinting*), nmap envía una serie de paquetes TCP y UDP, y examina cada bit de todas las respuestas del host objetivo, luego los compara con la base de datos nmap-os-db, donde se encuentran las respuestas conocidas e infiere el tipo de sistema operativo y su versión. En algunos casos, no se obtiene como resultado información demasiado precisa, por ejemplo nmap puede indicar que el host es un

Linux con versión de kernel en el rango 2.6.13 a 2.6.20. La opción indicada para realizar la identificación del SO es –O.

Cuando se ha encontrado un puerto abierto, se puede identificar la versión del programa que esté ofreciendo un servicio en dicho puerto (opción: -sV).

También incluye opciones que permiten evadir firewalls o IDS´s, como por ejemplo la fragmentación de los paquetes (opciones: -f ; --mtu), disimular el escaneo mediante señuelos (opción: -D), es decir, realizar el escaneo de puertos de tal manera que parezca que se está realizando al mismo tiempo desde varias IP´s (dichos señuelos deberán de encontrarse activos, en caso contrario se podría causar un ataque de inundación de paquetes SYN), suplantación de dirección IP (opción: -S) para hacer creer al host objetivo que el escaneo se ha originado desde un equipo ajeno al real, selección de la interfaz de red por la cual realizar el escaneo (opción: -e), también se puede especificar el puerto origen desde el cual mandar el escaneo (opción: --source-port), se puede indicar el número de bytes del paquete que se envíe (opción: --data-lenght), se pueden especificar distintos parámetros en los paquetes IP para poder manipular la ruta hacia cierto host (opción: --ip-options), indicar el valor del campo de tiempo de vida TTL de IP (opción: --ttl), realizar escaneos aleatorios de un conjunto grande de hosts para evitar posibles detecciones (opción: --randomize-hosts), suplantar la dirección MAC en las tramas Ethernet (opción: --spoof-mac), enviar paquetes con valores de checksum TCP/UDP inválidos (opción: --badsum), así como ajustar el retraso entre cada intento que se realiza a un determinado host (opción: --scan-delay).

Ejemplos:

#nmap -sL 10.0.0.1-3

Se obtienen los nombres de los hosts de las IP´s 10.0.0.1, 10.0.0.2 y 10.0.0.3

#nmap -v -sTUV -P0 -p 23,80,139 192.168.0.10

Con la opción –v (verbose), se incrementa el nivel de información que nmap entrega a la salida. La opción –sTUV indica que realizará un TCP SYN Scan, un UDP Scan, y se identificarán los programas y versiones que estén escuchando en el puerto, con –P0 se refiere a que no realice un ping inicial. Sólo se escanearán los puertos 23, 80 y 139. El host objetivo es el 192.168.0.10

#nmap -O --source-port 80 10.0.0.254

Aquí se intenta la identificación del sistema operativo del host 10.0.0.254, todos los paquetes que se envían, parecerán que son originados del puerto 80

#nmap -sN --scan-delay 1s -p 21-25,53 172.16.0.2

El escaneo será de tipo TCP NULL, con un retraso de 1 segundo entre cada paquete enviado. Sólo se revisarán los puertos 21, 22, 23, 24, 25 y 53 del host 172.16.0.2

Mediante estas técnicas, un atacante, fácilmente puede tener una idea bastante buena de la topología, servicios y tipos de hosts que se tienen en una red.

- **Buffer Overflow**

También llamado desbordamiento de buffer, consiste en aprovechar la vulnerabilidad de ciertos programas que no cuentan con controles adecuados que eviten que éstos reciban información de más y sobreescriba información destinada a áreas de datos destinadas para otros fines del programa. Es decir, se da en aplicaciones que no han sido programadas de manera correcta o que no cuentan con mecanismos de control que lo eviten (actualmente en la mayoría de los lenguajes de programación existen controles sencillos que permiten librarse de este tipo de problemas, pero aún existen programadores que no hacen uso de éstos).

Esta técnica, se utiliza frecuentemente en penetraciones de red remotas, donde un usuario anónimo en Internet busca obtener un control parcial o total de un sistema.

Tiene como objetivo alterar las funciones de un programa con privilegios suficientes, así el atacante obtendrá el control de éste y entonces logrará el control del host. Usualmente, se busca atacar un programa con privilegios de root o de administrador, e inmediatamente ejecuta algún código que le haga tener acceso a un shell. Para que pueda realizarlo, se deben de lograr dos objetivos previos: disponer de código adecuado en el espacio de direcciones del programa (por ejemplo exec(sh)) y hacer que el programa salte a ese código en memoria.

Hay dos formas de lograr tener código vulnerable en el espacio de direcciones del programa: inyectarlo o que éste ya se encuentre desde un principio dentro del código del programa

atacado, es decir, que el programa haga un uso legítimo de dicho código, por lo que el atacante puede aprovecharlo.

En caso de inyección de código, el atacante suministra una cadena de caracteres como entrada al programa atacado, y éste la almacena en un buffer que no es lo suficientemente grande para manejarla. La cadena de caracteres contiene instrucciones codificadas, usualmente en lenguaje ensamblador.

Se busca entonces alterar el flujo del programa para que se brinque a la dirección donde se encuentra el código del atacante. Para lograrlo, se desborda un buffer (ingresando más información de lo que puede almacenar por ejemplo, en un arreglo) para alterar partes adyacentes del programa, como por ejemplo direcciones de memoria.

Una vez que se haya logrado que el apuntador del programa tenga como valor la dirección de memoria con el código del atacante, fácilmente se puede tomar control de la máquina objetivo.

- **Código Malicioso**

Se llama código malicioso a los programas o scripts utilizados para realizar un ataque. Se puede clasificar en:

- Virus

Existen muchas definiciones de lo que es un virus informático, por ejemplo la de Matt Bishop: "Un virus informático es un programa que se inserta a sí mismo en uno o más archivos y luego realiza alguna acción", o Cohen: "Un programa que se replica infectando otros programas, para que así éstos contengan una copia de si mismo", existen otras definiciones más formales, como la propuesta por Guillermo Mallén: "Un virus es un conjunto de secuencias de símbolos, que cuando son interpretadas en un medio ambiente determinado, tienen la propiedad de hacer aparecer otra secuencia de símbolos perteneciente al conjunto de virus en otra parte del sistema". Se observa que lo que caracteriza a un virus es su capacidad de replicarse y no se hace referencia a los daños que pueden llegar a ocasionar. Esto se da en lo que se llama *payload* del virus, que puede ir desde una broma, hasta por ejemplo formatear el disco duro, borrar archivos vitales del Sistema Operativo, instalar puertas traseras, destrucción de información, saturación de recursos, bloqueo de equipos, etc., dependiendo de la imaginación y habilidades del autor del virus.

Pueden existir daños colaterales (efectos causados por el virus, pero que no fueron escritos para provocarlos), como por ejemplo con el virus Slammer (lanzado el 25 de Enero de 2003), que por su tasa de infección tan alta (durante el primer minuto de la epidemia, duplicaba el número de hosts infectados cada 8.5 segundos, al término de 3 minutos existían 55 millones de equipos contagiados, probó la totalidad de direcciones IP en aproximadamente 10 minutos y alcanzó 55 millones de escaneos por segundo) saturó el backbone de Internet provocando que muchos routers colapsaran, por lo que detuvo el tráfico de todo Internet alrededor de una hora. Cabe destacar que el Slammer no contenía ningún payload malicioso, su única función era infectar los hosts vulnerables (explotaba un a vulnerabilidad de buffer overflow en equipos con Microsoft SQL Server o con Microsoft SQL Server Desktop Engine 2000, sólo 75000 aproximadamente).

Utilizan una gran variedad de vectores de infección, como la utilización de correo electrónico, redes P2P, chats, páginas web maliciosas, propagación por medios extraíbles, aprovechamiento de vulnerabilidades en protocolos y programas, etc.

Existen 4 generaciones de virus a lo largo de la historia:

- 1ra. Generación: Son detectables a simple vista. Por ejemplo el histórico virus Ping Pong, que mostraba una pequeña "pelotita" que rebotaba alrededor de todo el monitor. Aparecía tanto en modo texto (en código ASCII) como en modo gráfico.
- 2da. Generación: Detectables con mecanismos propios del Sistema Operativo y utilerías. No realizan acciones que los delate de alguna manera evidente. Por ejemplo un archivo de texto será de tamaño mucho mayor, después de ser infectado, por lo que podría darse cuenta de su contagio notando el cambio en tamaño.
- 3ra. Generación: Son detectables con herramientas especializadas relativamente simples. Un ejemplo de esta Generación es el virus Anna Kournikova, que se reproducía auto enviándose a todos los contactos de Outlook que tuviera la máquina contagiada, ahora ya es detectado por la gran mayoría de programas antivirus existentes.
- 4ta. Generación: Detectables mediante algoritmos especializados en cada virus. Son los llamados virus polimórficos, produciendo cada vez que se reproducen un virus diferente.

Debe hacerse notar que a las infecciones por virus, aunque se den de manera relativamente frecuentes, se les acredita una serie de incidentes que no están relacionados siquiera con dicho

problema. Una gran tendencia es la de responsabilizar a un virus de cualquier daño o malfuncionamiento de los equipos.

También hay que tener en cuenta que la mayoría de los usuarios normales creen que la seguridad informática sólo se reduce en disminuir los contagios por virus y no ponen la debida atención o desconocen por completo las demás facetas involucradas.

- Ataques de Penetración

Para que un atacante logre exitosamente un ataque de penetración, deberá de cubrir con dos etapas: la penetración inicial y mantener una puerta trasera abierta.

La etapa de penetración inicial puede darse de muchas formas distintas, como por ejemplo la explotación de errores de diseño en protocolos de comunicación o programas de uso cotidiano, la utilización de virus, sniffers, o vulnerabilidades conocidas.

En la segunda etapa, el atacante asegura contar con una entrada al sistema que esté siempre disponible. Lo logra modificando o sustituyendo tanto programas como archivos de configuración, también puede instalar programas propios de ataque. Muchos de estos programas son llamados *rootkits*, por ejemplo se puede sustituir el programa ls de los sistemas operativos tipo UNIX, de manera que al listar una carpeta donde se hayan instalado programas maliciosos, éstos no aparezcan en el resultado de la ejecución, por lo que los usuarios del sistema no se darán cuenta de que existen.

Si un administrador se da cuenta de que su equipo ha sido comprometido, la labor de remover las puertas traseras que haya instalado el atacante no es trivial, ya que se pudieron haber colocado varias de éstas, además de que muchas veces el atacante se asegura de que no se puedan retirar, colocando mecanismos que, al detectar que se quieren extraer, realizan acciones destructivas, que llegando a inutilizar el equipo.

- Programas de Espionaje

Es software que es instalado secreta o sigilosamente en un equipo por el atacante, para recopilar información sin consentimiento de su dueño. Puede ingresar a un sistema por medio de cookies, entradas del registro de Windows incluso con archivos ejecutables.

Pueden llevar un registro de lo que se ingresa a través del teclado y enviar dicha información a una cuenta de correo o un servidor remoto (*keyloggers*), realizar capturas de la pantalla, encender el micrófono local vía remota, realizar seguimientos de las páginas por las que se navega.

El tipo que más prevalece actualmente es el *spyware*, éste es utilizado para fines comerciales. Existe una variante de spyware, que es el *adware*, cuya principal meta es la de mostrar constantemente publicidad de acuerdo a los hábitos del usuario.

También existen los llamados *caballos de Troya*, que consisten en programas que aparentemente realizan una función, como un salvapantallas o un juego, pero que en segundo plano efectúan actividades maliciosas. Un ejemplo es el *Back Orifice*, que utiliza el puerto 31337 tcp, instala un software servidor que se levanta cuando se enciende la computadora objetivo, mediante el cual el atacante puede manipular casi cualquier actividad de manera remota.

Existen los llamados *sniffers*, son programas que pueden observar y registrar el tráfico de una red. Su funcionamiento consiste en poner la tarjeta de red desde donde se lance el ataque, en modo promiscuo (en lugar de que la tarjeta sólo escuche el tráfico que va dirigido hacia ella, indicado por su dirección MAC, escucha todo el tráfico que circule por el medio). Pueden ser utilizados para propósitos benignos, como optimizar una red. Mediante dichas herramientas, se pueden por ejemplo obtener fácilmente listas de nombres de usuarios y contraseñas que viajan por la red en claro, es decir, viajan sin cifrar, por lo que cualquiera que esté monitoreando el tráfico puede leerlos directamente de los paquetes, también se puede saber qué sitios son los que accede determinado usuario, obtener los archivos que se envían y reciben, observar conversaciones de chat, etc.

- Bombas de Tiempo

Usualmente los virus contienen en su payload una bomba de tiempo, que son activados cuando se da cierto evento (generalmente una fecha y hora definidas), realizando actividades maliciosas.

Son utilizadas por empleados en descontento para sabotear sistemas. Igualmente son empleados en ataques de denegación de servicio (dichos ataques se explican más adelante en el capítulo).

Lo que da la dimensión del problema que ocasiona el código malicioso, es que por lo general, se lanzan ataques que son una mezcla de distintas técnicas, por lo que no es tan fácil mitigarlos, ya que se tiene que hacer uso de varias herramientas (programas antivirus, antispyware, detectores de integridad de archivos, sniffers, entre otros), además de la difícil labor de convencer a los usuarios de librarse de malos hábitos (por ejemplo, abrir todos los archivos adjuntos de cualquier correo que le llegue a su cuenta, aunque no conozca al remitente).

- **DoS (Denial of Service)**

Consisten en la inhabilitación de acceso a recursos de una red o sistema para usuarios legítimos de éstos. También se toma como ataque DoS, al retraso en operaciones críticas, como por ejemplo causar un aumento en la latencia en redes que utilizan servicios que requieren alta calidad como por ejemplo videoconferencias.

Se pueden utilizar distintas técnicas para llevar a cabo un DoS, como tratar de inundar una red con tráfico no legítimo, interrumpir la conexión entre dos equipos, evitar que cierta máquina tenga acceso a un servicio, invalidar a un usuario del mismo, agotamiento de recursos, etc.

Los DoS pueden ser clasificados en tres categorías:

- El consumo de recursos escasos, limitados o no reutilizables.

Se busca agotar o estropear recursos necesarios, tales como ancho de banda, espacio en disco y en memoria, tiempo del procesador, estructuras de datos, accesos a otros equipos o redes, potencia eléctrica, hasta el ventilador del CPU.

Usualmente su objetivo es la conectividad. Un ejemplo es el ataque conocido como *SYN Flood*, que consiste en que el atacante inicia el proceso de establecimiento de una conexión (three-way handshake), pero no llega a completarla. Como se envían un número muy grande de paquetes SYN, las conexiones válidas se ponen en cola de espera en lo que el equipo puede despachar los intentos de conexión dados.

También se puede generar una gran cantidad de errores en un servidor, que se grabarán en bitácora, buscando que estos archivos aumenten muchísimo su tamaño, agotando el disco.

- Destrucción o alteración de configuraciones

Por ejemplo, si el atacante logra corromper las tablas de ruteo de un equipo, éste no tendrá conectividad. En general, si se logra alterar la integridad de los archivos de configuración de un host, fácilmente se puede lograr que un una red o sistema no esté disponible.

- Destrucción física o alteración de componentes de red.

En esta categoría, se busca penetrar la seguridad física de una máquina, equipo activo, racks, segmentos del backbone de la red, energía eléctrica y cualquier otro componente crítico.

Otros ejemplos de DoS conocidos son: *Smurf Attack* (el atacante envía demasiados paquetes ICMP echo request, como si fuera un ping, a direcciones de broadcast; dichos paquetes tienen como dirección IP origen la del objetivo a atacar. Por lo que todos los equipos que se encuentren en el dominio de broadcast enviarán paquetes ICMP echo reply a la víctima), el *Fraggle Attack* (muy similar al *smurf attack*, sólo que utiliza paquetes *echo* UDP), el *Teardrop Attack* (aprovecha la fragmentación de los paquetes IP, envía fragmentos a la víctima, algunos duplicados, por lo que algunos equipos no saben cómo reensamblarlos), *Ping of Death* (se envían paquetes ping, normalmente de 64 bytes, mayores a 65535 bytes, por lo que puede saturar el buffer). Actualmente es muy fácil evitar todos estos ejemplos de DoS, pero aún es usual encontrar en la red algunos hosts que son vulnerables.

- **DDoS (Distributed Denial of Service)**

Es una técnica de ataque de denegación de servicio, que hace uso de un gran número de hosts para realizar el ataque. Se hace uso de esta técnica, porque actualmente el ancho de banda disponible es muy grande para muchas organizaciones.

Típicamente utilizan dos tipos de componentes: los *agentes* y los *manejadores*.

Los agentes, son programas que corren en hosts comprometidos, que envían tráfico malicioso a un mismo objetivo, basado en instrucciones (qué, cuándo y cómo atacar) de los manejadores. Existen casos en que no son necesarios los manejadores, el atacante se puede comunicar directamente con los agentes mediante otras técnicas, como por ejemplo canales IRC o los agentes ya saben desde un principio las acciones que deberán de realizar.

En los DDoS, los atacantes hacen uso de cientos o miles de equipos comprometidos, usualmente mediante código malicioso, para llevar a cabo el ataque.

Dos ejemplos de DDoS son el *Tribal Flood Network Attack* y el Trinoo. El TFN puede suplantar la dirección IP de origen para los agentes y puede realizar distintos ataques, como UDP Flood, ICMP Directed Broadcast, ICMP Echo Request Flood y TCP SYN Flood. Con el trinoo, el atacante se conecta a los manejadores mediante TCP usando telnet, éstos se conectan a los agentes a través del puerto 27444 UDP.

En la actualidad la mayoría de los equipos con salida a Internet, son potencialmente vulnerables a ataques DDoS, ya que ahora se hacen uso de los llamados *bots*, que serán explicados a detalle más adelante.

- **SQL Injection**

Aprovechando las malas o nulas verificaciones de los datos que son ingresados a distintos sistemas, se puede lograr acceder, alterar, insertar o borrar información a la que no se está autorizado.

SQL (Structured Query Language) es un lenguaje de consulta estructurado utilizado en bases de datos relacionales, mediante el cual se pueden realizar distintas operaciones en éstas. Entonces las aplicaciones que hacen uso de SQL, pueden ser objetivo de ataques de inyección de código.

Si el atacante provee como entrada parámetros especialmente elaborados, combinados con el servicio de Web de una aplicación, se generará una consulta SQL definida para atacar la confidencialidad y/o integridad de la base de datos.

Mediante las consultas, se puede llegar a obtener información, por ejemplo de nombres de campos, de tablas, usuarios válidos (listarlos, borrar o añadirlos).

Las bases de datos son tremendamente vulnerables a ataques, más aún, si éstas se encuentran en una aplicación web. Deberán de tomarse ciertas precauciones para mitigar el problema, como realizar una correcta validación, limitar la longitud de lo que ingresa un usuario, si se requiere realizar consultas acotar el número de éstas (por ejemplo mediante la creación de botones para cada consulta), filtrar ciertas palabras y caracteres que son utilizados en las

consultas, correr el servidor en una cuenta con pocos privilegios, entre otras. Aunque estas prácticas no harán a la base de datos cien por ciento segura, si lograrán que un atacante necesite emplear mayores recursos para poder afectarla.

- **Spam**

Es correo electrónico, con motivos comerciales o publicitarios, que es enviado masivamente a destinatarios que no lo han solicitado.

Puede llegar a colapsar un servidor de correo, o simplemente demorar la entrega de correos legítimos.

Según un estudio de Symantec, durante el 2008 el porcentaje del correo considerado como spam alcanzó entre un 75% y 85% del total de los correos enviados. Existen distintas categorías de spam: las relacionadas a temas de internet, salud, fraudes, temas adultos, financieros, engaños, ventas y ocio.

Actualmente, existe la venta de CD´s con listas de direcciones de correo, o incluso se vende el servicio de envío de spam.

Con una conexión de velocidad promedio, actualmente pueden enviarse hasta 12 millones de correos no deseados al mes.

El ancho de banda de las redes, frecuentemente es desperdiciado en el tráfico de este tipo de correos.

También, es difícil de rastrear, ya que muchas veces el atacante realiza el envío desde equipos que ya ha comprometido previamente.

Existe actualmente diversa tecnología antispam, como el filtrado por contenido en servidores de correo, la publicación de listas negras de spammers conocidos, listado de IP´s dinámicas, bloqueo de puertos (Prodigy tiene por default bloqueado el puerto 25) o utilizar técnicas para evitar la obtención de correos electrónicos en Internet (por ejemplo, en lugar de ingresar dentro del código de una página un correo electrónico, incluirlo como una imagen, así un programa que recopile automáticamente direcciones de correo de páginas de internet no podrá obtenerlo).

- **Phishing**

Se trata del engaño a los usuarios para revelar información personal sensible, a través del uso de alguna estafa. Se busca que el usuario se dirija hacia sitios web fraudulentos.

Usualmente utilizan el envío de spam para llegar a las víctimas. Se ha calculado que los atacantes que utilizan phishing, han logrado convencer hasta un 5% de los destinatarios (resulta negocio, debido al volumen masivo de correos enviados) a proporcionar información sensible, como números de cuenta, logins, contraseñas, números de tarjetas de crédito, PIN´s, números de seguridad de tarjetas de crédito (al reverso de éstas), números de netkey, etc.

Los sitios web fraudulentos son creados a manera de que parezcan sitios legítimos, mediante el uso de imágenes y hojas de estilo corporativas del sitio original. Usualmente se busca disfrazar la liga maliciosa, por ejemplo, en lugar de colocar www.bankofthewest.com, se coloca www.bankofthevvest.com, o se coloca www.banarnex.com, en lugar de www.banamex.com

Otra forma de ocultar la dirección maliciosa es la de incluir el carácter @ (los navegadores ignoran todo lo anterior a éste caracter), incluir la dirección IP convertida en un decimal (por ejemplo, a la IP 192.168.1.1 le corresponde el decimal: 3232235777), además de ocultar las extensiones de las páginas (por ejemplo .htm, se puede ocultar la letra t con su correspondiente en ASCII que es el 116, en hexadecimal es el 0x74, por lo que quedaría: .h%074m). Con esto se oscurece la dirección IP a la que se busca que la víctima ingrese. Por ejemplo:

http://www.banamex.com@3232235777/cuenta.h%074m

Un esquema de phishing, usualmente es el siguiente:

- El atacante envía un correo a la víctima, donde se le intenta hacer creer que debe de dirigirse hacia un sitio indicado. Se busca engañar al usuario, frecuentemente mediante avisos de mantenimiento o cambios en sistemas, la actualización de información personal, o incluso algún aviso de problemas de seguridad en su cuenta.
- Luego, cuando la víctima accede al sitio web malicioso, se le indica que ingrese la información que se busca obtener.
- Una vez que se tiene la información, ésta la puede obtener el atacante para realizar una transacción, o mediante un programa automático en el servidor malicioso realizarla.

En México, los sitios más atacados son los de Banamex, Bancomer, Banorte y American Express

Se pueden tomar distintas medidas en contra del phishing, como por ejemplo concientizar a los usuarios de eliminar los correos que no hayan solicitado, no redirigirse a sitios que no parezcan legítimos, nunca introducir información sensible en sitios web que no cuenten con un certificado digital válido, el uso de correo con firma digital, entre otros.

- **Pharming**

Similar al phishing. También conocido como DNS Poisoning, el pharming manipula los componentes de sistemas de dominios y resolución de nombres para dirigir a las víctimas a sitios maliciosos, que se encuentran bajo el control del atacante.

Se basan en técnicas de explotación a los DNS´s como por ejemplo: lograr obtener acceso a un servidor DNS y alterar la integridad de sus archivos de configuración; detectar las peticiones DNS y responder con los sitios que le interesa que la víctima ingrese, todo antes de que el verdadero servidor logre contestar; incluir la información requerida en un servidor DNS envenenando su caché, entre otros.

También pueden alterarse los archivos locales en un equipo, donde se hacen referencia de hostnames o alias, con su correspondiente IP. En sistemas operativos tipo UNIX, dicha información se encuentra en el archivo /etc/hosts, en sistemas tipo Windows se localiza en %Systemroot%\System32\Drivers\Etc\hosts

Puede mitigarse dicho ataque con técnicas similares usadas contra el phishing. Además de algunas específicas como mantener actualizados los servidores DNS, la verificación de resolución de nombres por un tercero (barras de herramientas en browsers, certificados digitales) y controles en los buscadores de Internet.

- **Cross Site Scripting (XSS)**

El XSS es una vulnerabilidad encontrada en aplicaciones web, que permite la inserción de código malicioso. Dicho código puede insertarse en la base de datos o en un archivo del servidor web, comúnmente utilizada en sitios de libros de visitas, blogs y cualquier otro donde se admite que los visitantes ingresen comentarios o información que luego podrán ver otros usuarios. Entonces está dirigido a atacar a los usuarios de un sitio web, no a los servidores en sí.

Sirve al atacante para insertar cualquier tipo de código (HTML, Flash, JavaScript, VBScript, etc) con lo que se puede realizar casi cualquier cosa que permitan los lenguajes utilizados. Mayormente, se utiliza el XSS para el robo de cookies (para, por ejemplo obtener nombres de usuario y contraseñas).

El ataque se da entonces, cuando la víctima, en un navegador, da click sobre la liga o simplemente se carga automáticamente por la existencia de algún script (malicioso de tipo onload).

Por ejemplo, al insertar el siguiente código en un sitio web vulnerable, se logrará que se abra una ventana de alerta en el navegador donde se indicará la leyenda “Sitio Vulnerable a XSS”:

<script>alert(´Sitio Vulnerable a XSS´);</script>

Aunque este código no realiza en sí nada malicioso, puede servir para comprobar que un sitio es vulnerable, por lo que es susceptible a que se inserte cualquier tipo de código.

Se puede minimizar el XSS mediante el filtrado de lo que pueda ingresar un usuario en un sitio web, por ejemplo, no permitir que se inserten los caracteres ´<´ y ´>´.

- **Suplantación**

La suplantación consiste en asumir la identidad de otra entidad.

Existen distintos tipos de suplantación, la más común es la suplantación de IP, que se refiere al envío de paquetes de red, que aparentemente provienen de una fuente distinta que la que en realidad la está enviando.

Normalmente se asocia el término de suplantación de IP a esconder la IP mientras se navega por Internet, chatea, envía correos, etc. Este concepto generalmente no es cierto. Ya que el alterar la dirección IP causa que el tráfico de vuelta no regrese satisfactoriamente, por lo que no se podrá establecer una conexión (completar el three-way handshake).

Puede utilizarse en casi cualquier tipo de ataque, por ejemplo, realizar un DoS al host con la IP legítima, esto es, el atacante espera a que el equipo atacado se desconecte de la red, entonces se conecta éste con la IP suplantada, por lo que al querer acceder a la red, el equipo verdadero no tendrá el servicio.

No sólo puede realizarse una suplantación de IP, también de direcciones MAC, DNS, de páginas web, de tablas ARP o de correo electrónico.

- **Web Defacement**

También llamado Cyber Graffiti. Se trata de un ataque a un sitio web que altera la apariencia de éste, o incluso suplantan todo el site.

Usualmente los atacantes colocan imágenes que hacen referencia al autor, o a leyendas políticas.

Existen sitios que llevan las estadísticas del número de defacements comprobados que ha realizado un hacker (clasificado por su seudónimo), o de los países que mayor número de sites han alterado.

- **ARP Poisoning**

El protocolo ARP permite asociar direcciones MAC con IP´s. Aprovecha que no existe ninguna autenticación en dicho protocolo y que es posible el envío de respuestas ARP no solicitadas. Por lo que cualquier equipo en una LAN puede suplantar a otro equipo en la misma LAN.

El atacante crea paquetes ARP reply para que los equipos donde se colocará en medio, guarden en su tabla ARP su dirección MAC para cierta IP. Por lo que cualquier tráfico que se transmita entre dichos hosts tendrá que pasar por el atacante, antes de que llegue al otro host legítimo, entonces se puede interceptar o manipular el tráfico en tránsito.

Éste es un tipo de ataque conocido como Hombre en Medio, que son ataques a protocolos de autenticación donde el atacante se posiciona entre la entidad que realiza una petición y la entidad que lo verifica, para así poder interceptar y alterar la información de la comunicación entre éstas dos.

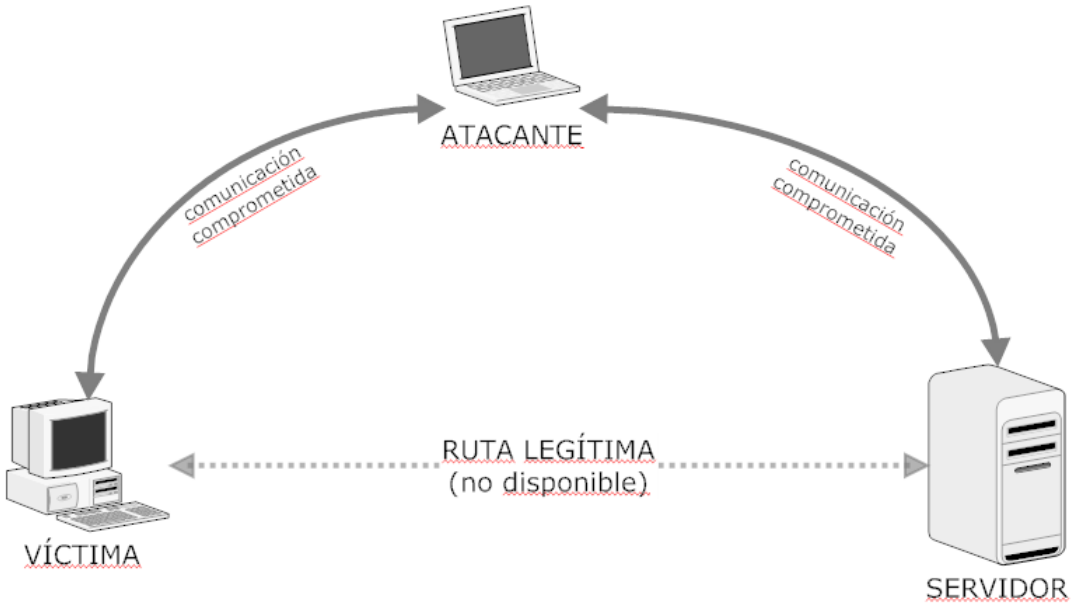


Figura 1.10 Ataques Hombre en Medio

- **Password Cracking**

El atacante busca obtener o descifrar contraseñas de usuarios legítimos en un sistema. Normalmente se buscará obtener una contraseña de un usuario con privilegios.

Puede utilizar técnicas tan distintas como la observación de lo que los usuarios ingresan en el teclado, inferencia (intentar adivinar las contraseñas basándose en información que se tiene acerca del usuario, como fecha de nacimiento, gustos, nombres de familiares, o cualquier cosa que pueda usarse como contraseña), software dedicado, ataques de fuerza bruta (se intentan todas las combinaciones del espacio de contraseñas posibles, es muy lento, pero estadísticamente sólo se tienen que probar la mitad del espacio para acertar), ataques de diccionario (se recorre un diccionario de palabras previamente creado, incluso existen varios disponibles en Internet, dicho diccionario deberá de tener ciertas características para aumentar la posibilidad de hallarla, por ejemplo el lenguaje utilizado).

Entre el software existente, los más utilizados (según insecure.org) son:

- **Cain & Abel**. Es una herramienta de recuperación de passwords de Windows. Puede monitorear el tráfico en una red, usa ataques de diccionario, de fuerza bruta, realiza criptoanálisis, graba conversaciones de VoIP, revela contraseñas guardadas por navegadores y analiza distintos protocolos.
- **John the Ripper**. Es una herramienta rápida y multiplataforma. Principalmente se utiliza para detectar contraseñas débiles en sistemas UNIX. También soporta los passwords tipo hash de UNIX, Kerberos y Windows NT/2000/XP.
- **THC Hydra**. Busca obtener contraseñas de autenticación de redes, y distintos protocolos, como telnet, FTP, HTTP, HTTPS, SMB, bases de datos, entre otros.
- **Aircrack**. Utillizado para obtener llaves WEP/WPA.
- **L0phtcrack**. También conocido como LC5. Realiza las mismas funciones que Cain & Abel, o John the Ripper.
- **Airsnort**. Obtiene llaves WEP de los protocolos 802.11. Muy similar a Aircrack.
- **SolarWinds**. Contiene un buen número de herramientas de descubrimiento de redes, monitoreo y de ataque.
- **Pwdump**. Se utiliza para extraer hashes NT y LANMAN de equipos Windows.
- **Rainbow Crack**. Realiza ataques de fuerza bruta cientos de veces más rápidos que otro tipo de herramientas.
- **Brutus**. Sólo trabaja bajo Windows. Realiza ataques de fuerza bruta y de diccionario a los protocolos HTTP, POP3, FTP, SMB, telnet, entre otros.

- **Bots y Botnets**

La utilización de miles de equipos para realizar un ataque DDoS se ha convertido en un ataque muy recurrente en la actualidad.

Entonces se tiene que crear previamente al ataque una red de máquinas zombies (llamada Botnet), usualmente se busca controlar máquinas con un buen ancho de banda, y son infectadas por código malicioso controlado remotamente. Ahora se están utilizando canales de IRC para el control y manejo de los hosts infectados. Son utilizadas también para el envío de spam, montar servidores de software pirata, seriales, crack, robo de información sensible, distribución e instalación de malware.

Incluso se ha logrado detectar la primer botnet para equipos MAC (comúnmente ajeno a las amenazas de seguridad), llamada *iBot*, en abril del 2009.

Existe un mercado negro de bots, e incluso se llegan a alquilar las botnets para un ataque específico. Las botnets son uno de los principales recursos de los atacantes en la actualidad.

- **Zero Day´s**

Cuando se encuentran vulnerabilidades de ciertos sistemas o aplicaciones y éstas no han sido publicadas (por lo mismo no existen parches o mecanismos de detección), pueden ser explotadas sin ningún problema. Usualmente pasan unos cuantos días desde que se descubre una vulnerabilidad y se publica, por lo que en este tiempo los sistemas no cuentan con ninguna protección.

También puede referirse como Zero Day, a los virus que no han sido descubiertos y aún no son detectables por ningún motor de búsqueda de software antivirus.

- Ingeniería Social

La ingeniería social aprovecha la mayor de las vulnerabilidades de cualquier sistema: el ser humano.

Un sistema puede contar con los mecanismos de seguridad más avanzados, pero al final un atacante puede obtener la información que deseé simplemente con una llamada a un empleado desprevenido o que no tenga conciencia de lo que la ingeniería social consiste.

Ésta se refiere al uso de distintas acciones para conseguir información proveniente de personas cercanas a un sistema, que atente contra éste. Hace uso de distintas características del ser humano como las relaciones personales, inocencia, curiosidad, credibilidad, arrogancia, morbo, codicia, miedo, ignorancia, etc. También puede utilizarse el chantaje, la amenaza, o algún otro medio para que las víctimas cooperen aún en contra de su voluntad.

Incluso el usuario más experto y con vastos conocimientos sobre seguridad informática, es susceptible a la ingeniería social.

Una de las prácticas más comunes de los ingenieros sociales, es la de simplemente realizar una llamada haciéndose pasar por gente de mantenimiento, o soporte y enredar a la víctima para

que le entregue información. También puede hacer simples observaciones, utilizar chats, hacer *dumpster diving* (recolección de información a partir de documentos desechados), escuchar conversaciones, hacerse pasar por un usuario nuevo, o por alguien a quien un usuario normal acudirá en caso de problemas (*reverse social engineering*), hacer uso de las redes sociales, o cualquier cosa que la inventiva del atacante piense.

La forma de disminuir el problema de la ingeniería social es la educación, tanto de los usuarios normales, como de los administradores. También deberán de existir procedimientos establecidos y separación de responsabilidades, para que aunque un usuario haya sido víctima de un ingeniero social, éste no pueda llevar a cabo su ataque sin tener que atacar a otra persona.

Los ataques descritos anteriormente son sólo unos cuantos de los existentes. Nos sirve para darnos una idea de que los sistemas y aplicaciones son vulnerables a ataques muy variados.

Hay que tener en cuenta que un sistema deberá de tener procedimientos, políticas y mecanismos de seguridad que disminuyan la probabilidad de que todos los ataques a los que es vulnerable no se lleven a cabo. Mientras que los atacantes sólo tienen que encontrar un único camino para llegar a dañarlo, usualmente utilizan la vía más corta, por lo que hay que colocarles obstáculos para que deban de gastar más recursos informáticos para vulnerarlo, así si el costo de la información a obtener es menor que el costo de obtenerla, el atacante tendrá que preguntarse si vale la pena continuar y dedicar los recursos y el esfuerzo necesarios, o simplemente intentar por otras alternativas.

1.6 TIPOS DE CONTROLES DE SEGURIDAD

Un control de seguridad es una protección o contramedida, ya sea de tipo *técnico, de gestión u operacional*, colocados en un sistema de información para la protección de la confidencialidad, integridad, disponibilidad, autenticación y no repudio de dicho sistema y su información.

- **Técnicos**. Los controles de seguridad técnicos para la mitigación de riesgos pueden configurarse para proteger los activos contra cierto tipo de amenazas. Usualmente hay que tener en cuenta las arquitecturas de los sistemas, software, hardware y firmware. Existen tres tipos de controles técnicos: de apoyo, preventivos y de detección, así como de recuperación

- **De Apoyo.**

Son requeridos para que otros controles puedan ser implantados correctamente. Son los siguientes:

- **Identificación**. Proporcionan la habilidad de identificar usuarios, procesos y activos de información. Deben estar debidamente identificados tanto sujetos, como objetos.
- **Manejo de Llaves Criptográficas**. Cuando se han implantado funciones criptográficas en otros controles, las llaves criptográficas deberán de ser administradas de manera segura, ya que si se llegan a vulnerar o a divulgar, toda la criptografía del sistema se invalidará. Incluye la generación, distribución, almacenamiento y mantenimiento de las llaves.
- **Administración de Seguridad**. Se deberán de activar o desactivar las características de seguridad de un sistema de las Tecnologías de Información (TI), con el fin de satisfacer las necesidades de seguridad de éste. Pueden encontrarse dichas características en los sistemas operativos o en las aplicaciones utilizadas. Por ejemplo, la habilitación de vigencia de cuentas, de políticas de contraseñas robustas, de conexiones remotas, etc.
- **Protecciones de Sistema**. Como fundamento de las capacidades funcionales de seguridad de cualquier sistema, se encuentran las implantaciones técnicas, desde el punto de vista de los procesos utilizados de diseño y en la forma en que se llevó a cabo la implantación. Pueden ser, por ejemplo, la protección de los objetos de reuso, privilegios mínimos, separación de procesos, modularidad y minimización de objetos confiables.

- **Preventivos.**

Pueden inhibir intentos de violaciones de las políticas de seguridad. Incluyen:

- **Autenticación**. Brindan los medios para la verificación de la identidad de un sujeto, para el aseguramiento de que la entidad que dice ser, sea válida. Abarcan las contraseñas, números de identificación y tecnologías de autenticación como tokens, smart cards, certificados digitales, kerberos, biometría, entre otros.
- **Autorización**. Permite la especificación y gestión de las acciones permitidas en un sistema.

- **Actualización de Control de Acceso**. Cuando un sujeto que solicita acceso a un recurso, ha sido autorizado es necesaria la actualización de la política de seguridad que se refiere al control de acceso (por ejemplo discrecional o mandatoria).
- **No repudio**. El no repudio se extiende tanto a prevención como detección, es un elemento fundamental en las auditorías de sistemas. Estos controles, usualmente son colocados en los puntos de transmisión o recepción de información.
- **Protección de Comunicaciones**. En sistemas distribuidos, la correcta implantación de los servicios de seguridad depende en gran medida en el grado de confianza de las comunicaciones. Se debe de proteger la información cuando se encuentra en tránsito. Incluyen las VPN´s, IPSEC, criptografía de llave pública y funciones hash.
- **Privacidad de Transacciones**. Incluyen protocolos como Secure Socket Layer (SSL) y Secure Shell.

- **De Detección y Recuperación**

Los controles técnicos de detección, alertan sobre posibles violaciones o intentos de violar las políticas de seguridad.

Los controles técnicos de recuperación son utilizados para la restauración de activos perdidos.

- **Auditoría**. Una correcta auditoría de eventos importantes relacionados con la seguridad, en conjunto con un correcto monitoreo y seguimiento de éstos, son elementos esenciales en un análisis forense posterior y una eventual recuperación.
- **Detección y Contención de Intrusos**. La oportuna detección de los incidentes de seguridad, es muy importante para una correcta reacción en tiempos adecuados que permitan reaccionar debidamente. Si se da la detección de un incidente y no se pueden efectuar las medidas correspondientes ante éste, la detección no es de gran ayuda, por lo que este tipo de controles deberán de trabajar conjuntamente.
- **Verificación de Integridad**. Analizan la integridad en un sistema y detectan violaciones en éste y ayudan a una correcta determinación de la medida a tomar en caso de un incidente.
- **Restauración a un Estado Seguro**. Permite regresar el sistema a un estado conocido y seguro, después de que ha ocurrido un incidente.

- **Detección y Eliminación de Software Malicioso**. Programas que detecten, identifiquen y eliminen software malicioso instalado en servidores, y estaciones de trabajo, para ayudar a asegurar la integridad de un sistema y su información.

- **De Gestión**. Los controles de seguridad de gestión, en conjunto con los técnicos y los operacionales, son útiles para un adecuado manejo y reducción de riesgos relacionados con pérdidas y para la protección de la misión de la organización. Estos controles tienen como objetivo principal la implantación de políticas de seguridad, guías y estándares, que deberán de ser implantados en todos los aspectos operacionales de la organización. Se dividen en:

  - **Preventivos.**

  Incluyen los siguientes controles:

  - Asignación de responsables de seguridad.
  - Desarrollo y mantenimiento de programas de seguridad, que documenten los controles que se tienen y se pueda planear a futuro la implantación de otros.
  - Implantación de controles de seguridad del personal, como la separación de responsabilidades, mínimos privilegios, acceso a personal nuevo y revocación de privilegios a personal que ya no labore en la organización.
  - Llevar a cabo labores de concientización del personal.

  - **De Detección.**

  Incluyen los siguientes controles:

  - Controles de seguridad en el personal, por ejemplo la terminación de empleados, investigación de antecedentes y rotación de deberes.
  - Revisiones periódicas de los controles, para asegurar su efectividad.
  - Realización de auditorías de forma periódica.
  - Efectuar una gestión de riesgos.
  - Identificación y autorización o rechazo de riesgos residuales.

- **De Recuperación.**

Incluyen los siguientes controles:

- Desarrollo y mantenimiento de Planes de Continuidad de Negocio (BCP).
- Desarrollo y mantenimiento de Planes de Recuperación de Desastres (DRP).

- **Operacionales**. Los estándares de seguridad en una organización deberán de establecer un conjunto de procedimientos que sirvan para una correcta implantación de las metas de la misión. La dirección es clave en el establecimiento y cumplimiento de las políticas, mediante controles operacionales apropiados.
- Mediante los controles operacionales, se pueden llegar a corregir ciertas deficiencias operacionales que podrían llegar a ser aprovechadas por ciertas amenazas. Por lo que se deberá de elaborar documentación que contenga procedimientos detallados paso a paso y métodos claramente definidos, minuciosos y actualizados. Se clasifican en:

- **Preventivos.**

Incluyen los siguientes controles:

- Control de acceso a medios y su correcta eliminación, por ejemplo el manejo del control de acceso físico.
- Limitación de distribución de datos a externos, por ejemplo la utilización de etiquetas.
- Control sobre software antivirus.
- Salvaguardar las instalaciones de cómputo, por ejemplo guardias de seguridad, procedimientos para personal externo o visitantes, biometría, manejo y distribución de llaves, entre otros.
- Aseguramiento de equipo activo.
- Proveer capacidad de respaldos al interior y fuera de sitio
- Establecimiento de procedimientos de respaldo fuera de sitio.
- Protección de equipo de cómputo, tanto móvil como fijo.
- Protección contra incendios, por ejemplo requerimientos y procedimientos de uso de extintores.
- Procedimientos de restablecimiento de electricidad en caso de fallas.
- Controles de humedad y temperatura en instalaciones de cómputo.

- **De Detección.**

Incluyen los siguientes controles:

- Seguridad Física. Por ejemplo uso de sistemas de circuito cerrado.
- Seguridad del ambiente de trabajo. Por ejemplo detectores de humo.

1.7 EJEMPLOS DE MECANISMOS DE SEGURIDAD

A continuación se explicarán algunos mecanismos de seguridad:

- **Firewall**

Un firewall es un dispositivo o sistema que manipula el flujo de tráfico entre redes. Existen diferentes tipos, cuyas capacidades pueden ser comparadas basándose en el modelo OSI, es decir, indicando en qué capas pueden ser manejados.

Los firewalls operan en las siguientes capas:

- Capa 7 Aplicación. (Clientes de correo, navegadores, aplicaciones en general)
- Capa 4 Transporte. (Puertos TCP o UDP)
- Capa 3 Red. (Direcciones IP)
- Capa 2 Enlace. (Direcciones MAC)

Mientras más avanzado sea el firewall, más capas podrá abarcar, por lo que serán más efectivos en su tarea.

Los distintos tipos de firewalls existentes actualmente son: filtrado de paquetes, inspección de estados, puertas de enlace con proxy de aplicación, servidores proxy dedicados, híbridos y basados en host.

- **Filtrado de paquetes**

Son los más comunes, son esencialmente dispositivos de ruteo con funcionalidades de control de acceso que se rigen por un conjunto de directivas conocidas como reglas, que controlan el flujo según:

- *Dirección de origen* del paquete (capa 3, Red).
- *Dirección de destino* del paquete (capa 3, Red).
- *Tipo de tráfico* (capas 2 y 3), es decir, el protocolo de red específico utilizado en la comunicación de las entidades origen y destino.
- *Puertos de origen y destino* (capa 4).
- *Interfaces de red.*

Estos parámetros pueden usarse en cualquier combinación para establecer el conjunto de reglas. Además se debe de indicar la acción a realizar cuando un paquete coincide con una, como aceptarlo (se deja pasar el paquete a su destinatario), denegarlo (no se permite el paso al paquete, y un mensaje de error es enviado a la entidad que lo generó) o deshacerse de él (igual que la denegación, pero no regresa ningún mensaje de error), así como mandarlo o no a bitácora.

Deben de contar con una política o postura general al momento de crear el conjunto de reglas. Puede adoptarse una política permisiva: "Todo lo que no está específicamente prohibido está permitido"; o una política paranoide: "Todo lo que no está específicamente permitido está prohibido"

El orden de las reglas también es importante, ya que al momento de que llegue un paquete, se intentará coincidir con alguna regla, inspeccionando de una a una hasta que se ajuste a una de ellas. En caso de que no coincida con ninguna, la acción dependerá de la política adoptada.

Los firewalls de filtrado de paquetes pueden operar a grandes velocidades (sólo limitada por el número de reglas que deberá de revisar para cada paquete).

Usualmente son colocados como firewalls de frontera en las proximidades de redes no confiables, donde podrán llegar a bloquear ciertos ataques, filtrar protocolos no deseados y realizar un primer control de acceso.

Los firewalls de filtrado de paquetes no previenen ataques dirigidos a vulnerabilidades o funciones de aplicaciones específicas, debido a que no examinan los paquetes en las capas más altas; también son vulnerables a ciertos ataques que toman ventaja de problemas en especificaciones TCP/IP, como la suplantación de IP.

- **Inspección de estados**

Son firewalls de filtrado de paquetes, que pueden procesar información que involucra conexiones y otros estados (como llevar el registro de actividad reciente por host o por conexión). Es decir, toma en cuenta en cuenta el estado de paquetes previos. También agrega la funcionalidad de inspeccionar las banderas de control TCP (URG, ACK, PSH, RST, SYN y FIN)

Una vez establecida una conexión válida (habiendo una coincidencia con una regla de estado), se podrá enviar cualquier tipo de tráfico.

- **Proxy de aplicación**

Combinan el control de acceso de capas inferiores con funcionalidades de capa 7 (aplicación). Implica el conocimiento de los protocolos utilizados por cada aplicación. Es en sí, un software que reenvía o bloquea conexiones basadas en aplicaciones. Analiza el paquete por completo, no sólo los encabezados como en el caso de los firewalls anteriormente descritos.

Cada proxy de aplicación, también conocido como agente proxy, interactúa directamente con el conjunto de reglas para determinar si cierto tráfico deberá de ser permitido o no, (por ejemplo permitir o no ciertos comandos). Además, pueden añadir autenticación para cada usuario de la red, que puede ser por ID de usuario y password, tokens (por software o hardware) o autenticación por dirección de origen.

El análisis detallado de los datos de aplicación, a menudo puede alentar la comunicación, ya que cada paquete debe de ser analizado de manera minuciosa

Pueden llevar una bitácora más detallada, ya que inspecciona todo el paquete, por ejemplo se puede mandar a registro los comandos utilizados.

Una desventaja de los proxys de aplicación es que están limitados en protocolos y aplicaciones de red nuevos. Se deberá de tener un proxy de aplicación para cada tipo de tráfico que se requiera (DNS, FTP, HTTP, HTTPS, SMTP, entre otros).

Existen los llamados *servidores proxy dedicados*, que controlan el tráfico de la aplicación (autenticación, registro), pero no contienen capacidades de firewall (capas inferiores). Son comúnmente utilizados para análisis de contenidos web y de correo.

Adicionalmente un firewall puede brindar servicios como NAT o DHCP.

NAT (*Network Address Translation*). Se desarrolló para abordar dos puntos importantes en redes y seguridad: el ocultamiento del esquema de red de los equipos detrás de un firewall y el agotamiento de las direcciones IP disponibles, por lo que se utilizan detrás del firewall direcciones IP privadas (especificadas en el RFC 1918). Puede llevarse a cabo de tres maneras distintas: NAT estático, NAT dinámico, Hiding NAT y PAT (Port Address Translation).

- *NAT estático.* Cada dirección IP en la red privada tiene una correspondiente dirección IP ruteable asociada. Es muy raro que actualmente se utilice. Por ejemplo:

Dirección IP Interna (Privada)	Dirección IP Externa (Ruteable)
192.168.0.1	201.10.0.51
192.168.0.2	201.10.0.52
192.168.0.3	201.10.0.53
192.168.0.4	201.10.0.54
192.168.0.5	201.10.0.55
192.168.0.6	201.10.0.56
192.168.0.7	201.10.0.57

Tabla 1.11 Ejemplo de NAT estático

- *NAT dinámico.* Idéntico al estático, sólo que la dirección privada se mapea a la primer dirección IP ruteable de un conjunto específico en el momento de querer establecer la comunicación.
- *Hiding NAT.* Todos los sistemas que se encuentran detrás del firewall comparten la misma dirección externa ruteable. Este tipo de traslación es muy común, ya que si se cuenta únicamente con una IP homologada, se puede dar servicio de red a un gran número de equipos.

Sin embargo, los sistemas con redes privadas no pueden poner a disposición recursos a usuarios externos (del otro lado del firewall).

Entonces, toda la actividad de los equipos detrás del firewall, parecerá (a sistemas externos) como si se originara desde la dirección IP ruteable (u homologada) del firewall. Un ejemplo se muestra en la figura 1.13

Segmento de direcciones IP Internas	Dirección IP Externa (Ruteable)
192.168.0.0/24	201.10.0.51

Tabla 1.12 Ejemplo de Hiding NAT

- PAT. También conocido como overloading. Se mapean todos los equipos con direcciones privadas de detrás del firewall, hacia una única IP homologada mediante el uso de distintos puertos. Por ejemplo:

Dirección IP Interna (Privada)	Dirección IP Externa (Ruteable)
192.168.100.1	200.0.100.51:101
192.168.100.2	200.0.100.51:102
192.168.100.3	200.0.100.51:103
192.168.100.4	200.0.100.51:104
192.168.100.5	200.0.100.51:105
192.168.100.6	200.0.100.51:106
192.168.100.7	200.0.100.51:107

Tabla 1.13 Ejemplo de PAT

DHCP (*Dynamic Host Configuration Protocol*). Permite a los equipos conectados en una red, obtener la configuración de red necesaria. Es un protocolo cliente-servidor, puede asignar las direcciones IP de manera estática (asignando una IP asociada a una dirección MAC específica) dinámica (asignando direcciones IP disponibles de un rango, sea de forma permanente o durante un tiempo determinado).

La colocación de un firewall constituye únicamente la primera línea de defensa contra ataques externos, usualmente se cree que sólo con un firewall se logra una seguridad adecuada, esto no es correcto ya que no es el único mecanismo. Una práctica aconsejable es la de aplicar el concepto de defensa en profundidad, donde se colocan una serie de firewalls en capas alrededor del esquema de red, para que así un ataque que venga desde fuera tenga que realizar un mayor esfuerzo para alcanzar su objetivo; al igual que en el caso de que un sistema detrás del firewall se vea comprometido (ya sea por un ataque o accidental) éste no pueda afectar los activos más importantes de la organización.

También se deberá mantener en constante actualización las reglas de filtrado para que se adecuen a los requerimientos de seguridad. Es recomendable tener un procedimiento para la inclusión de nuevas reglas

- **IDS e IPS**

Un IDS (Intrusion Detection System) es un software que busca actividades sospechosas en la red y alerta a sus administradores. Un IPS (Intrusion Prevention System) también detecta actividad intrusiva y además puede intentar detenerla, idealmente antes de que llegue a su objetivo.

Monitorean el tráfico en una red o bitácoras de auditoría de sistemas. Pueden detectar intrusiones que han logrado pasar por un firewall o que se estén suscitando en la red local detrás de éste.

Algunos pueden interactuar con firewalls, para así poder brindar un enfoque reactivo a la seguridad de una red.

Pueden clasificarse en: basados en host y basados en red.

- *Basados en Host*. Revisan el sistema y las bitácoras de eventos para así poder detectar un ataque al host y determinar si el ataque ha sido exitoso. Están limitados a las capacidades de registro en bitácoras del sistema. Sin embargo, son vulnerables a ataques que alteren la integridad del sistema que están monitoreando. Algunos ejemplos son: *Swatch* y *LIDS*.
- *Basados en Red*. Proveén información en tiempo real, sin tener que consumir recursos de red o de host. Se comporta de manera pasiva mientras recolecta datos. Revisa paquetes y sus

encabezados. Al ser el monitoreo en tiempo real, puede llegar a limitar un ataque. Un ejemplo de este tipo de IDS, es el más utilizado en la actualidad: *Snort*.

Cuentan con dos tipos de métodos de detección: basados en firmas y basados en anomalías estadísticas:

- *Basados en Firmas*. Cuentan con firmas o atributos que caracterizan un ataque, almacenados para su referencia. Los datos adquiridos, ya sea mediante bitácoras o por el análisis de paquetes de red son comparados con las firmas, si hay coincidencias se inicia una respuesta. Tienen como desventaja el necesitar grandes cantidades de información para poder detectar ataques que se extienden por mucho tiempo (que realizan cada paso del ataque en periodos muy distantes entre sí), también sólo puede detectar ataques de los que se tenga una firma como referencia.
- *Basados en Anomalías Estadísticas*. Se recolectan datos y se define un perfil de uso normal de la red o del host que se está monitoreando. Se incluye en la recolección, datos como utilización de memoria, de procesador y de tipo de paquetes de red. Con este esquema se pueden detectar ataques nuevos ya que producen estadísticas anormales. Tiene como desventaja el no poder detectar ataques que no cambien significativamente las características, o puede obtener falsos positivos con anomalías circunstanciales en el sistema.

Cuando se implanta un IDS o IPS, es natural que éste se convierta en un objetivo principal para ataques que busquen deshabilitarlos y permitan realizar las actividades maliciosas pasando desapercibidos. Son vulnerables a ataques de denegación de servicios y a ciertas técnicas de evasión de IDS e IPS, como la fragmentación IP o ataques vía TTL (alterando el valor de TTL para que el IDS vea paquetes que no llegarán al objetivo, así se insertan datos falsos y se puede enmascarar el verdadero ataque). También es común que, en el caso de ataques DoS, este tipo de sistemas lleguen a ser deshabilitados por el ataque mismo. Deberán de mantenerse actualizados para contar con las últimas firmas. Además, en el caso de detección por firmas, no logran descubrir ataques nuevos, de los cuales no se han elaborado sus firmas respectivas. También exigen una correcta administración, ya que en muchos casos se mandan alertas de falsos positivos.

Es recomendado implantar IDS basados en host en los sistemas críticos, aún a los que en teoría no puedan ser accedidos desde fuera. En general se deberán de colocar en cualquier lugar de la red donde se permita la entrada de tráfico de red de entidades externas.

- **Criptografía**

La criptografía es la ciencia de usar matemáticas para cifrar y descifrar datos. Permite el almacenamiento y transmisión de información crítica a través de redes inseguras como Internet, de manera que no pueda ser leída por personas no autorizadas.

Un algoritmo criptográfico es una función matemática utilizada en el proceso de cifrado y descifrado, trabaja en conjunto con una llave utilizada para cifrar el texto en claro. La fortaleza de un algoritmo criptográfico se mide por medio del tiempo y los recursos que se necesitarían para recuperar el texto en plano y de la robustez de la llave usada.

Las funciones de cifrado y descifrado, junto con la llave (K), el mensaje en claro (M) y el mensaje cifrado o criptograma (C), constituyen lo que se conoce como criptosistema.

Se denomina como criptoanálisis al proceso de intentar obtener el mensaje en claro, a través del mensaje cifrado, sin conocer la llave.

Existe el llamado Principio de Kerckhoff, que indica las reglas para que un sistema criptográfico sea considerado seguro, aunque se conozca en su totalidad (con excepción de la llave) los componentes de éste. Establece:

1. No debe de existir forma alguna de obtener el mensaje en claro o la llave, a partir del mensaje cifrado.
2. Todo sistema criptográfico deberá de contar con información tanto pública (algoritmos) como privada (llave).
3. La llave deberá ser fácil de recordar y de cambiar.
4. Los mensajes cifrados deberán de poder ser enviados por medios de comunicación habituales.
5. La complejidad del proceso de obtención del mensaje en claro, deberá de corresponderse con el beneficio obtenido.

La criptografía se clasifica, de acuerdo al número de llaves en: criptografía simétrica, criptografía asimétrica y función hash.

- *Criptografía Simétrica*. También llamada *criptografía clásica* o *de llave secreta*. Únicamente se utiliza una llave, tanto para el proceso de cifrado como para el descifrado. La seguridad depende de un secreto compartido entre el emisor y el receptor de la comunicación. Se basa en

dos métodos básicos: la confusión y la difusión. La *confusión* se aplica mediante sustituciones (corrimientos, simple, homofónica, polígrama o polialfabética) y la difusión mediante permutaciones (reordenamientos). Los algoritmos simétricos más fuertes son los llamados producto, que incluyen tanto operaciones de confusión como de difusión. Ejemplos de algoritmos de este tipo son: DES, IDEA, 3DES, AES

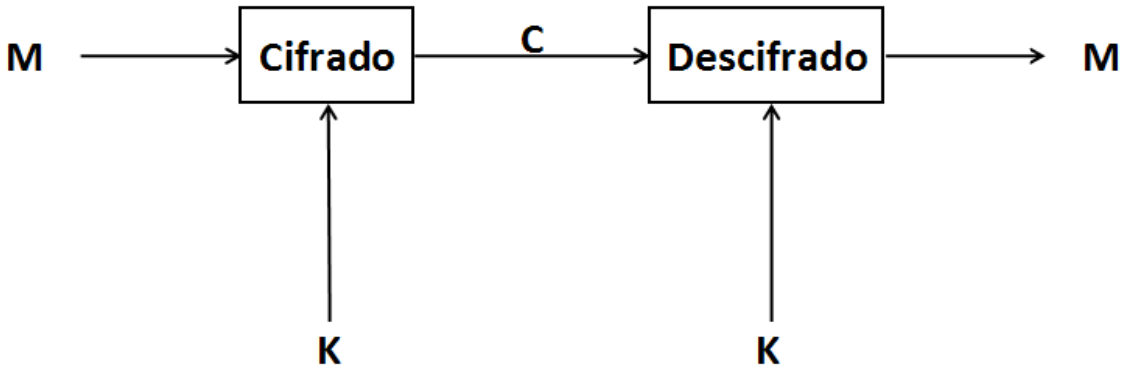


Figura 1.14 Criptografía Simétrica

- *Criptografía Asimétrica*. También llamada *criptografía de llave pública*. Nació a partir del paper publicado por Whitfield Diffie y Martin Hellman en el año de 1976, donde se propone un nuevo tipo de criptografía, así como se propone un algoritmo de acuerdo de llaves (Algoritmo Diffie-Hellman) y se da solución al problema de Firma Digital.

En este tipo de criptografía se utilizan dos tipos de llaves, una pública y una privada, generadas al mismo tiempo y relacionadas entre sí. Cualquiera puede realizar un cifrado utilizando una llave pública, pero sólo podrá descifrar el criptograma quien posea la llave privada.

Según Diffie y Hellman, los algoritmos de cifrado asimétricos deben de cumplir con las siguientes propiedades de viabilidad computacional:

1. Cualquier usuario puede calcular su propio par de llaves pública y privada.
2. El emisor puede cifrar con la llave pública del receptor en tiempo polinomial.
3. El receptor puede descifrar el criptograma con la llave privada en tiempo polinomial.
4. El problema de un criptoanalista que busque obtener la llave privada a partir de la llave pública, es de orden exponencial.

5. El problema de un criptoanalista que intente descifrar un criptograma conociendo la llave pública, es de orden exponencial

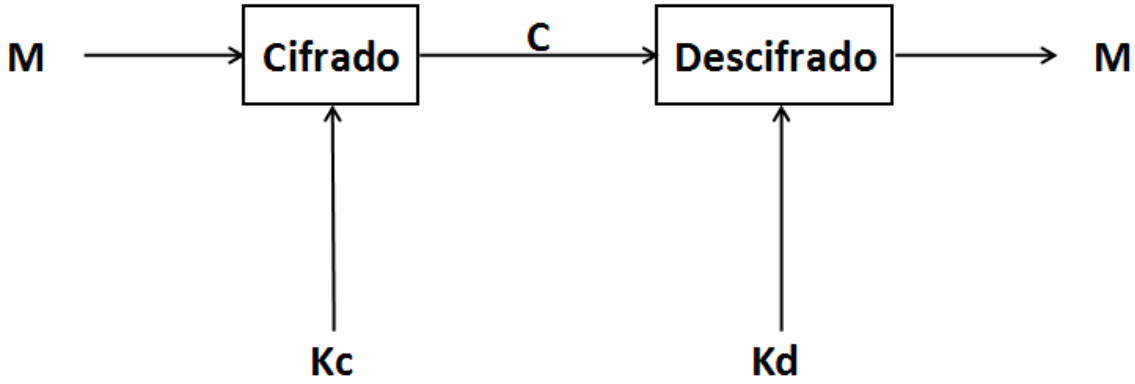


Figura 1.15 Criptografía Asimétrica

Mediante el uso de criptografía de llave pública, se pueden establecer comunicaciones sin que las dos partes hayan tenido contacto previo alguno.

Deberá de establecerse una infraestructura de llave pública (PKI, Public Key Infrastructure), para el aseguramiento de que las llaves públicas utilizadas sean válidas y así evitar ataques de hombre en medio.

Algunos ejemplos de algoritmos asimétricos son: RSA, El Gamal y acuerdo de llaves Diffie-Hellman.

En este tipo de criptografía se basa el concepto de *firma digital*, que consiste en una transformación por medio de una función de firma, que relaciona de forma única un archivo con dicha función y un elemento propio de la identidad del firmante (llave privada). Consiste de dos procesos: el proceso de firma y la verificación de ésta.

- *Función Hash*. Son funciones de un solo camino, es decir que una vez que se haya obtenido un valor hash, no existe función matemática alguna para obtener el mensaje original a partir de éste.

Las funciones hash son un resumen de la entrada, no es un cifrado de ésta.

Como entrada a las funciones hash se puede tener cualquier tipo de archivo o documento de cualquier longitud posible y como salida el valor hash es de longitud fija. De tal manera que si

la entrada cambia en al menos un solo bit, el valor hash resultante será uno distinto. En otras palabras, se tiene un universo de entradas o mensajes posibles a los que los corresponden sólo un valor hash dentro del universo de valores hash posibles definidos por el algoritmo.

Una buena función hash deberá de evitar colisiones, es decir, que dos o más entradas generen el mismo valor hash; o que una sola entrada pueda generar dos o más valores hash.

Pueden ser utilizados para la verificación de integridad de un documento o para la autenticación de usuarios.

Algunos ejemplos de algoritmos de funciones hash son: MD5, RIPEMD, y SHA.

Como resumen de los mecanismos de seguridad criptográficos y los servicios de seguridad que resguardan se tiene el siguiente cuadro:

SERVICIO DE SEGURIDAD	MECANISMO DE SEGURIDAD CRIPTOGRÁFICO
-Confidencialidad	- Cifrado Simétrico - Cifrado Asimétrico
- Verificación de Integridad	- Cifrado Simétrico - Función Hash
- Disponibilidad	*NO SE PUEDE GARANTIZAR
- Autenticación	- Cifrado Simétrico - Cifrado Asimétrico - Función Hash - Firma Digital
- Control de Acceso	- Modelos de control de acceso (DAC, MAC, RBAC y Optimista)
- No Repudio	- Firma Digital

Tabla 1.16 Servicios de seguridad resguardados por mecanismos criptográficos

- **Modelos de Control de Acceso**

La función del control de acceso es la de manejar qué entidades pueden acceder a ciertos recursos y qué pueden hacer sobre de éstos.

Existen mecanismos de control de acceso a nivel de hardware, de sistema operativo y de aplicación.

Se han desarrollado distintas formas de control de acceso: la discrecional, mandatoria u obligatoria, basado en perfiles y optimista.

- **Control de Acceso Discrecional (DAC).** En este tipo de control de acceso se establece un dueño para cada entidad (archivo, programa, aplicación, dispositivo, etc.) y él es el único que puede asignar o revocar permisos sobre ésta. Puede implementarse mediante el uso de bits de permiso, contraseñas, listas de capacidades o listas de control de acceso.

- *Bits de Permiso*. Cada archivo cuenta con sus propios permisos de sólo lectura, escritura y/o ejecución que otorga el dueño. Por ejemplo, en UNIX hay tres clases de usuario: el dueño, el grupo (al que pertenece el dueño) y los otros (cualquier usuario con acceso al sistema) y existen tres tipos de permisos: lectura, escritura y ejecución. Se asignan de la siguiente forma:

  rwxrwxrwx El primer bloque de permisos (r-read, w-write y x-execute) son para el dueño, el siguiente bloque es para el grupo y el último es para los demás usuarios.

- *Contraseñas*. El dueño asigna un password y lo divulga a los usuarios que puedan tener acceso. Es vulnerable a pérdida o divulgación no autorizada y cambios.
- Listas de Capacidades. Cada usuario tiene una lista que contiene los nombres de los objetos a los que tiene acceso y sus derechos. La lista la mantiene el sistema operativo y los usuarios no pueden tener acceso a la lista.

- Por ejemplo:

Archivo 1	Dueño, leer, escribir
Archivo 2	Escribir
Archivo 3	Ejecutar
Archivo 4	Leer, Escribir

- *Listas de Control de Acceso (ACL).* Cada archivo tiene una lista asociada, donde se encuentran los usuarios que pueden accederlo y sus permisos. Por ejemplo:

Juan	Leer, escribir
Pedro	Ejecutar
Paco	Leer, añadir

- **Control de Acceso Mandatorio (MAC).**

  El usuario no controla la autorización para acceder a objetos. Los usuarios cuentan con un nivel de autorización de acceso y la información es clasificada. Estos parámetros se combinan para crear las *clases de acceso*.

  Existen diversos modelos mandatorios, como el modelo *Bell-LaPadula, Biba y Clark Wilson.*

  - *Bell-LaPadula*. Resguarda la confidencialidad. No se puede leer desde arriba ni escribir hacia abajo. Además no puede haber más de un sujeto al mismo tiempo que pueda leer y escribir sobre un archivo.
  - *Biba*. Resguarda la integridad. Se asignan niveles de integridad a los sujetos y los objetos. Establece que no se puede escribir hacia arriba ni se puede leer desde abajo.
  - *Clark-Wilson*. También resguarda la integridad de la información. Verifica que los usuarios autenticados no modifiquen indebidamente la información, para lo que plantea la división de tareas para que éstos no realicen operaciones indebidas.

- **Control de Acceso Basado en Perfiles (RBAC).**

  Los permisos se otorgan a perfiles, no a usuarios específicos. Los usuarios no pueden otorgar ni revocar permisos. Los usuarios son catalogados por perfiles, según sus responsabilidades y capacidades. Puede cambiarse un usuario de perfil sin problema alguno. Pueden otorgarse o revocarse permisos a los perfiles sin modificar el control de acceso.

  El dueño de la información no es un usuario, sino la organización misma.

- **Control de Acceso Optimista**

  Es un modelo de control, donde el control es más relajado en comparación con los otros. Se confía en los administradores para evitar el abuso y se elaboran transacciones compensatorias para garantizar la integridad. Se elaboran procedimientos parciales compensatorios.

Para la correcta implantación de modelos de control de acceso se deberá de tener una buena certeza tanto de los sujetos y de los objetos que conforman la organización, además de su nivel dentro de ésta. Además se debe de complementar con una correcta autenticación (ya sea por conocimientos, posesión de objetos o características físicas), ya que si no se cuenta con ésta, el control de acceso no garantizará un nivel de seguridad óptimo.

- **Políticas de Seguridad**

Las políticas de seguridad son el conjunto de reglas por medio de las cuales se resguardan los servicios de seguridad en la medida que lo requiere una organización. Son el marco de referencia de la seguridad, en ellas se define lo que está permitido y lo que está prohibido, permiten definir procedimientos necesarios, responsabilidades y tareas.

Las políticas de seguridad son fundamentales en la administración de la seguridad de una organización. Deberán ser evaluadas periódicamente para que concuerden con la misión de la seguridad.

Se deberá de establecer una postura general al momento de la redacción de las políticas:

- *Paranoico*. Nada está permitido
- *Prudente*. Todo aquello que no esté expresamente permitido está prohibido
- *Permisivo*. Todo aquello que no esté expresamente prohibido está permitido
- *Promiscuo*. Todo está permitido

En el momento de que ocurra un incidente de seguridad, las políticas indicarán quiénes tienen la debida autoridad para tomar acciones que mitiguen el impacto de éste y evitar que se repita. Permiten identificar y eventualmente sancionar a los responsables.

Para una correcta redacción de las políticas, se deberá de conjuntar un equipo, incluyendo a la alta administración, conformado por personal que tenga la experiencia y capacidad necesaria para la tarea.

Se deberá de indicar el alcance de las políticas al inicio del proceso de redacción, que sea consistente con la misión de seguridad de la organización.

Asimismo, deberán de contener ciertos rubros como la definición de la seguridad, objetivos, importancia, un enunciado de la intención de la dirección de la organización, un marco referencial (incluyendo una breve descripción de la gestión de riesgos), consecuencias de la violación de alguna política y referencias.

Se debe también de tomar en cuenta que las políticas que no sean del todo aceptadas por los usuarios, serán difíciles de implantar, a menos que se indiquen sanciones que logren el cumplimiento de éstas a pesar de contar con una aceptación entusiasta.

Al final, no deberá contarse con políticas que afecten la productividad o la misión de la organización.

Debe de indicarse en cada política los responsables, las acciones y los periodos de validez, es decir quién, qué y cuándo.

Deben considerarse ciertos puntos de importancia organizacional como: protección y clasificación de los recursos, separación de funciones, monitoreo, mínimo privilegio, redundancia, continuidad, actualización, cultura, ética, administración y mejores prácticas.

La adopción de un mecanismo de seguridad deberá ser justificado por una o más políticas. Todo control deberá de contar con procedimientos de operación, administración y contingencia.

Se deberá de evitar que las políticas sean inconsistentes entre sí y evitar contradicciones.

Todos los usuarios deben de leer y firmar de aceptación sobre las políticas de seguridad antes de otorgárseles acceso a los recursos.

Entre algunas de las políticas necesarias en una organización se tienen que tomar en cuenta:

- *Políticas de uso aceptable*. Indican qué es lo que puede y no puede hacerse con los recursos de cómputo, así como responsabilidades, permisos, cuándo compartir cuentas de usuario, uso de correo electrónico, páginas web, etc.
- *Políticas de cuentas de usuario*. Determina los procedimientos para la adquisición de privilegios para usuarios y su vigencia. Además de definir quiénes tendrán la autoridad de otorgarlos o revocarlos. Indican también los derechos y deberes de los usuarios, políticas de vigencia e inhabilitación de cuentas y el proceso de desecho de éstas (manejo de información que tuvieran dichas cuentas de usuarios).
- *Políticas de acceso remoto*. Se definen los métodos aceptados para realizar conexiones desde fuera de la organización. Asimismo establecer quiénes tienen éste derecho.
- *Políticas de protección de la información*. Buscan evitar que se altere o difunda información sensible durante procesos, transmisiones y almacenamiento.
- *Políticas de configuración de firewalls*. Establece responsabilidades sobre el establecimiento y cambios de configuración, además de quiénes tienen acceso a éstos y procesos de mantenimiento de acuerdo a las necesidades de la organización.
- *Políticas de cuentas privilegiadas*. Establece quiénes tendrán acceso a cuentas con privilegios, procedimientos de auditoría de dichas cuentas y condiciones para la cancelación de dichos accesos.
- *Políticas de conexión a la red*. Indican los requisitos necesarios para que un dispositivo pueda ser conectado a la red, también se especifican quiénes pueden instalar nuevos recursos de red, definir quiénes lo autorizan y documentación de cambios.

Una vez que se han elaborado las políticas de seguridad, es necesario elaborar los procedimientos de seguridad que indiquen cómo es que se tendrán que llevar a cabo. Dichos

procedimientos constituyen los mecanismos para hacer cumplir las políticas. Tendrán que ser lo más detallados y específicos posibles. Algunos procedimientos que se requieren son:

- Auditorías de seguridad.
- Administración de cuentas.
- Administración de autenticadores.
- Administración de la configuración de sistemas.
- Respaldos de datos y programas.
- Manejo de incidentes.
- Escalamiento de problemas.
- Planes de respuesta a desastres.

Las políticas de seguridad también deberán de ser sometidas a revisión en periodos establecidos o en la ocurrencia de cambios significativos en la organización. Para la correcta realización de la revisión, se deberá de tener en cuenta lo siguiente:

- Retroalimentación de los usuarios
- Resultados de revisiones independientes
- Resultado de revisiones previas
- Desempeño
- Tendencias de seguridad
- Incidentes reportados
- Recomendaciones de autoridades

CAPÍTULO 2. METODOLOGÍA DE RESOLUCIÓN DEL PROBLEMA

Se realizará un estudio de gestión de riesgos, como resultado se tendrá una serie de controles de seguridad que buscarán mitigar los riesgos encontrados, además de una lista de los riesgos residuales identificados.

La metodología de gestión de riesgos utilizada será la propuesta por el *National Institute of Standards and Technology (NIST)*, en la publicación especial *SP 800-30 "Risk Management Guide for Information Technology Systems"*. Fue escogida debido a que se acopla a los fines de esta tesis, permitiendo una gestión de riesgos cualitativa cuyos procesos se encuentran perfectamente detallados, es ampliamente utilizado en organizaciones que requieren de estudios serios y profundos en rubros de seguridad de la información (por ejemplo el Banco de México), no dan lugar a interpretaciones, como resultado parcial arroja una serie de controles recomendados para la disminución de los riesgos identificados y es de uso libre; y como resultado final se especifican los controles idóneos para mitigar dichos riesgos; además de dar las pautas para una constante revisión de los resultados obtenidos. En el punto 3.4.1 se explica a detalle esta metodología.

Diversas metodologías de gestión de riesgos fueron descartadas como opción a utilizar, debido a desventajas como las siguientes:

- *OCTAVE*. Se eliminó debido a que está diseñado para organizaciones de más de 300 empleados. Podría aplicarse esta metodología con el conjunto de criterios mencionados en el método OCTAVE-S, diseñado para organizaciones pequeñas, pero se encuentra aún en fase de desarrollo. Además OCTAVE tiene como objetivo final la realización de estrategias de toma de decisiones que buscan disminuir los riesgos, más que a la selección de controles de seguridad.
- *ISO 27005*. Es propietario, la licencia cuesta entre 150 y 200 dólares. Además de que no define si el estudio a realizar se hará con un enfoque cualitativo o cuantitativo, se deja a consideración de quienes lo efectúan. Está enfocado a fungir como apoyo a la certificación ISO 27001.
- *Magerit*. Esta metodología fue descartada debido a su enfoque cuantitativo, se le asigna un valor a cada activo a analizar, por lo que puede llegar a extenderse el tiempo del análisis. Además en la DCB es casi imposible la asignación de valores monetarios a los activos, debido a que su principal objetivo es educativo.

Como apoyo, se hará uso del estándar *ISO 27002*, que propone una serie de controles de seguridad y está diseñado para satisfacer los requerimientos identificados mediante un análisis de riesgos.

Dicha documentación aunque es propietaria y se requiere de pagar licencia, puede encontrarse en línea para usos académicos en: http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

En la figura 2.1 se muestra un esquema de la metodología a emplear.

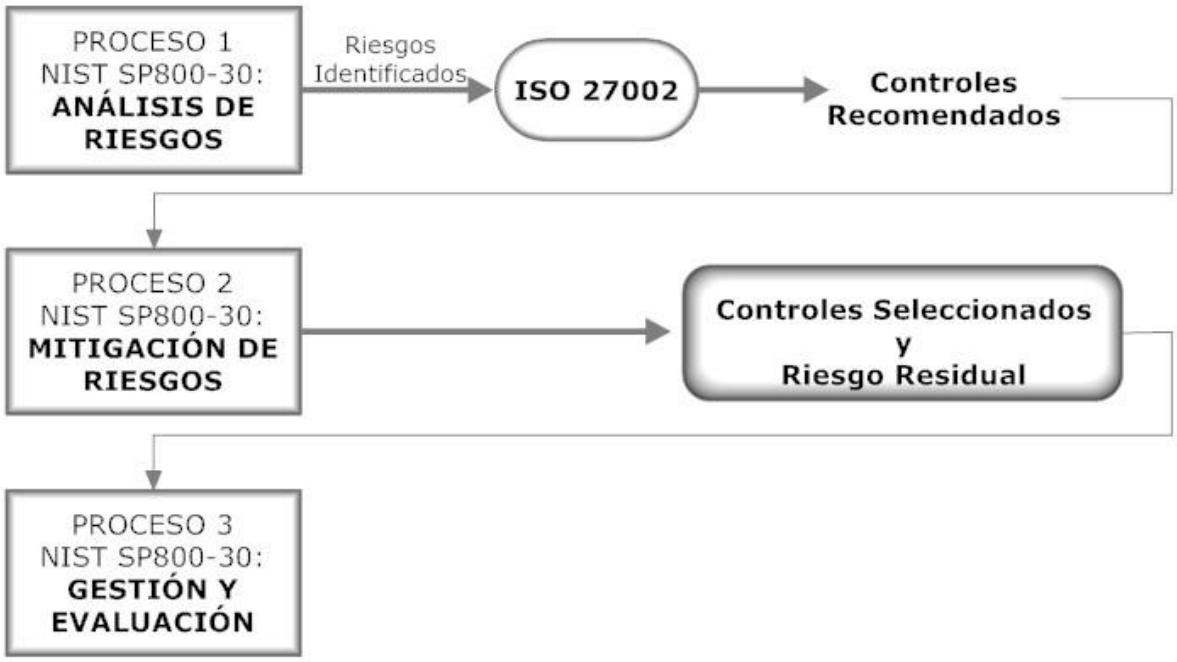


Figura 2.1 Metodología propuesta

2.1 NIST SP 800-30

El National Institute of Standards and Technology (NIST), es una agencia federal, dependiente del Departamento de Comercio de los Estados Unidos, fundada en 1901 cuya misión es elaborar y promover patrones de mediciones, estándares y la tecnología con el fin de innovar la productividad y facilitar el comercio.

Las Publicaciones Especiales (Special Publications, SP) de la serie 800, son una serie de documentos de interés general para la comunidad de seguridad en cómputo. La serie SP 800 fue

establecida en 1990 para suministrar una alternativa en publicaciones de información de tecnologías de la seguridad en cómputo.

Entre los documentos más relevantes de la serie SP800 se encuentran:

- **SP 800-12**. El Manual del NIST. Una Introducción a la Seguridad de la Información
- **SP 800-30. Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información**
- **SP 800-41**. Guía para Implantación de Firewalls y Políticas de Firewalls
- **SP 800-45.** Guía para la Seguridad de Correo Electrónico
- **SP 800-47**. Guía de Seguridad para la interconexión de Sistemas de Tecnología de la Información
- **SP 800-57**. Recomendaciones para la Gestión de Llaves Criptográficas
- **SP 800-61**. Guía para el Manejo de incidentes de Seguridad
- **SP 800-68**. Guía para el Aseguramiento de Sistemas Microsoft Windows XP para Profesionales de las Tecnologías de Información
- **SP 800-69**. Guía para el Aseguramiento de Microsoft Windows Home Edition: Una Lista de Verificación de Configuraciones de Seguridad
- **SP 800-83**. Guía de Prevención y Manejo de Incidentes con Malware
- **SP 800-92**. Guía para la Gestión de Bitácoras de Seguridad
- **SP 800-94**. Guía para Sistemas de Detección y Prevención de Intrusos
- **SP 800-95.** Guía para Servicios de Web Seguros
- **SP 800-100**. Manual de Seguridad de la Información. Guía para Administradores
- **SP 800-111**. Guía para las Tecnologías de Almacenamiento Cifrado para Dispositivos de Usuario Final
- **SP 800-123**. Guía de Seguridad de Servidores en General

A continuación se describe la metodología propuesta en el NIST SP800-30 "Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información".

Consta de tres grandes procesos, mediante los cuales se identifican primero los riesgos, luego se realizan actividades que buscan disminuir el impacto en caso de éstos, finalmente actividades que realizan revisiones periódicas.

Figura 2.2 Procesos del NIST SP800-30

- **EVALUACIÓN DE RIESGOS**

La evaluación de riesgos o análisis de riesgos, es el primer proceso que se realiza en la metodología de gestión de riesgos. Distintas organizaciones la utilizan para la determinación del grado de amenazas potenciales y el riesgo asociado a un sistema de TI. Los resultados de este proceso son una herramienta para la identificación de controles de seguridad apropiados para la reducción o eliminación de riesgos durante el proceso de mitigación de los mismos. Dicho proceso cuenta con 9 pasos, descritos en la figura 3.3

- ***Paso 1. CARACTERIZACIÓN DEL SISTEMA***

Cuando se realiza un análisis de riesgos, el primer paso es la definición del ámbito al cual será aplicado, es decir identificar los límites del sistema de TI que será el objeto de nuestro análisis, así como los recursos con los que cuenta y la información que constituye el mismo.

La caracterización de un sistema de TI, nos dice el alcance de la gestión de riesgos que le será implementada, las autorizaciones operacionales (o permisos), y también nos brinda información esencial para la definición de los riesgos, como por ejemplo el hardware, software, conectividad, personal encargado, etc.

- La identificación de un riesgo requiere de un pleno entendimiento del ambiente del proceso del sistema. Quienes realizan el análisis de riesgos deberán de recolectar antes que nada información relativa al sistema, que usualmente es clasificada como sigue:

- Hardware
- Software
- Interfaces del sistema (conectividad tanto interna, como externa)
- Información y datos
- Personal que mantiene y utiliza el sistema
- Misión del sistema
- Nivel crítico del sistema y los datos
- Sensitividad del sistema y los datos

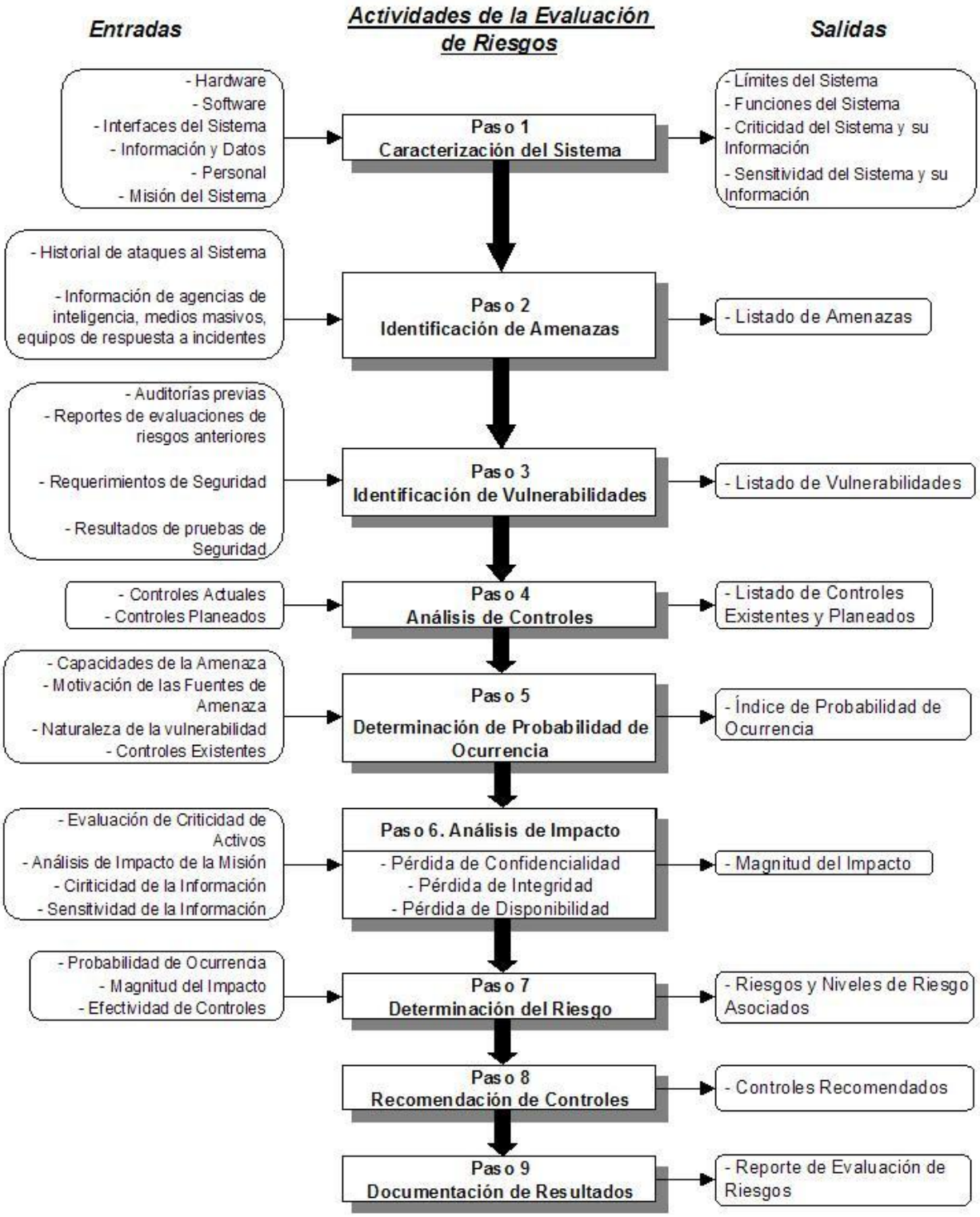


Figura 2.3 Actividades de la Evaluación de Riesgos

También puede incluirse:

- Requerimientos funcionales del sistema
- Usuarios
- Políticas de seguridad del sistema a las que está sujeto el sistema
- Arquitectura de seguridad
- Topología de red
- Protección del almacenamiento de la información
- Controles técnicos utilizados por el sistema
- Controles de gestión del sistema
- Controles operacionales
- Entorno de seguridad física

Si el sistema se encuentra en fases de inicio o de diseño, la información puede derivarse de los documentos de diseño y requerimientos del mismo. Si el sistema se encuentra en desarrollo, es necesario definir reglas y atributos de seguridad planeados para su implementación en un futuro. Los documentos del diseño y plan de seguridad (en caso de que exista) pueden proveer información útil acerca de la seguridad de un sistema de TI que se encuentra en desarrollo.

Para un sistema de TI que ya se encuentre en operación, la información se recolecta en el entorno de producción, incluyendo in formación en configuraciones, conectividad, procedimientos y prácticas, ya sea que se encuentren documentadas o no. Por lo que la descripción del sistema puede basarse en la seguridad que provee la infraestructura subyacente o en planes de seguridad a futuro para el sistema.

Existen distintas técnicas de recolección de información como cuestionarios, entrevistas en sitio, revisión de documentación y utilización de herramientas de escaneo automático.

- *Resultados obtenidos de la Caracterización del Sistema:* Un buen panorama del ambiente donde se encuentra el sistema, y la delineación de los límites de éste.

- ***Paso 2. IDENTIFICACIÓN DE AMENAZAS***

Una amenaza no presenta riesgo alguno cuando no existe una vulnerabilidad que pueda ser utilizada.

Cuando se determina la probabilidad de un riesgo, deberá considerarse el origen de las amenazas, las vulnerabilidades potenciales y los controles existentes.

Se deberán de identificar las amenazas potenciales y realizar una lista de éstas, que puedan ser aplicables al sistema de TI que se está estudiando.

Cuando se evalúan los orígenes de las amenazas, se deberán de considerar todas aquellas que podrían causar daños al sistema de TI y a su ambiente de proceso. Por ejemplo, en la ciudad de México hay una alta incidencia de sismos, por lo que deberá de tomarse en cuenta dicha amenaza natural.

El ser humano es considerado como un origen de amenazas, ya que sus acciones pueden conducir a un ataque deliberado, por desconocimiento, o por error,. Por ejemplo:

Un ataque intencionado se puede dar de formas diversas, como intentos maliciosos para ganar accesos no autorizados a un sistema de TI, la obtención de contraseñas mediante herramientas o ingeniería social y así poder comprometer la integridad, confidencialidad y disponibilidad del sistema o de la información que maneja; también puede realizarse un intento bien intencionado, pero que con un propósito específico eluda la seguridad de un sistema, como por ejemplo que un administrador escriba un caballo de troya, que le permita saltarse la seguridad de su sistema, para así poder realizar más rápido su trabajo.

Las amenazas humanas son las que potencialmente son más peligrosas, debido a las distintas motivaciones y los recursos que podrían llegar a tener. La tabla presenta las amenazas humanas más comunes, con las posibles motivaciones que pudieran tener y las distintas acciones que pudieran llevar a cabo para proceder con un ataque.

Un estimado de las motivaciones, recursos y capacidades que pueden ser requeridas para llevar a cabo un ataque exitoso deberá de ser desarrollado después de que la identificación de las amenazas potenciales, esto, para poder determinar la probabilidad de que una amenaza explote una vulnerabilidad del sistema.

El listado amenazas potenciales, deberá de ser realizada específicamente para una organización y su ambiente de proceso. Por lo general, la información de amenazas naturales (por ejemplo, terremotos, tormentas, etc.) ya debe de encontrarse disponible en la organización. Existen amenazas que ya han sido identificadas por distintos gobiernos y organizaciones privadas. También se tienen al alcance varias herramientas de detección de intrusos. Se pueden tomar como fuentes de información (no son las únicas), las siguientes:

- Agencias de Inteligencia, por ejemplo el Centro de Protección de la Infraestructura del FBI de los EU
- El Federal Computer Incident Response Center (FedCIRC)
- Medios masivos, en particular los recursos basados en Web, por ejemplo páginas como SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, SANS.org, Cert.org

■ *Resultados obtenidos de la Identificación de Amenazas* La lista de amenazas potenciales que podrían llegar a explotar alguna vulnerabilidades del sistema

AMENAZA	POSIBLES MOTIVACIONES	ACCIONES
Hackers o crackers	- Reto - Ego - Rebelión	* Actividades de Hackeo * Ingeniería Social * Intrusiones al Sistema * Accesos al Sistema no autorizados
Criminales Informáticos	- Divulgación Ilegal de información - Destrucción de Información - Razones monetarias - Alteración de Datos no autorizada	* Crimen informático (por ejemplo, acoso por computadora) * Fraude (por ejemplo, robo de identidad) * Soborno * Suplantación * Intrusiones al Sistema
Terroristas	- Chantaje - Destrucción - Explotación - Venganza - Ultimátum - Boicot	* Terrorismo * Tráfico de Información * Manipulación del Sistema * Penetraciones al Sistema * Ataques al sistema (por ejemplo, una negación de servicio distribuida)
Espionaje Industrial (entre compañías, gobiernos, distintos intereses gubernamentales)	- Ventajas Competitivas - Espionaje Económico	* Explotación económica * Robo de Información * Intrusiones en la privacidad del personal * Ingeniería social * Penetraciones al Sistema * Accesos no autorizados al sistema (acceso a información clasificada, propietaria o relacionada a alguna tecnología)
Personal de confianza (mal entrenados, en descontento, maliciosos, negligentes, deshonestos o antiguos empleados)	- Curiosidad - Ego - Reto de Inteligencia - Razones monetarias - Venganza - Errores no intencionados u omisiones (por ejemplo, errores de programación)	* Asalto a empleados * Chantajes * Navegación a través de información propietaria * Abusos en el uso de cómputo * Fraudes y Robos * Código Malicioso (por ejemplo, virus, bombas lógicas o troyanos) * Colocación de información falsificada o corrupta * Intercepción * Sobornos * Venta de Información del Personal * Colocación de errores en la programación * Intrusiones al Sistema * Accesos no autorizados al sistema

Tabla 2.4 Amenazas humanas, posibles motivaciones y acciones

- ***Paso 3. IDENTIFICACIÓN DE VULNERABILIDADES***

Una *vulnerabilidad,* es una debilidad o falla en los procesos, diseño, implementación o controles internos de un sistema, que podrían ser ejercidos (accidentalmente desencadenada o intencionalmente explotada), resultando una violación en las políticas del sistema o en una violación de seguridad.

El objetivo de este punto es el desarrollo de una lista de vulnerabilidades (fallas o debilidades) que podrían llegar a ser explotadas por las amenazas potenciales.

Se deberá de realizar una lista de pares vulnerabilidad/amenaza como la siguiente:

Vulnerabilidad	Amenaza	Acción
Identificadores (ID) de empleados despedidos no son removidos del sistema	Empleados Despedidos	Acceso a la red de la organización, y acceso a información sensible
Firewall perimetral permite telnet entrante, y el ID guest está habilitado en el servidor patito.com	Usuarios no autorizados (hackers, empleados despedidos, criminales informáticos)	Utilización de telnet hacia el servidor patito.com y navegación por archivos no autorizados a través de la cuenta *guest*
Proveedores han identificado fallas en el diseño de seguridad del sistema; pero no se han aplicado parches al sistema	Usuarios no autorizados (hackers, empleados descontentos, criminales informáticos)	Acceso no autorizado a archivos de sistemas sensibles basados en vulnerabilidades conocidas del sistema
El Data Center utiliza rociadores de agua para reprimir fuegos; lonas para proteger hardware y equipo de daños del agua no se encuentran colocados	Fuego, personal negligente	Encendido de rociadores de agua en el Data Center

Tabla 2.5 Pares Vulnerabilidad/Amenaza

Algunos métodos recomendados para la correcta identificación de vulnerabilidades de un sistema son:

- Uso de fuentes de vulnerabilidades, como por ejemplo SANS.org, la base de datos de vulnerabilidades NIST I-CAT (icat.nist.gov), la National Vulnerability Database (nvd.nist.gov), la Open Source Vulnerability Database (osvdb.org), la base de datos del Cert (*www.kb.cert.org/vuls/*), entre otras. Avisos de seguridad, como el FedCIRC, o el boletín del Incident Advisory Capability del Department of Energy´s Computer de los EU. Así como avisos de proveedores.
- La realización de pruebas de rendimiento de la seguridad de un sistema.

  Las pruebas y evaluaciones de seguridad, son técnicas que pueden ser utilizadas para identificar vulnerabilidades en sistemas de TI, durante el proceso de evaluación de riesgos. Incluyen el desarrollo y ejecución de planes de pruebas, por ejemplo scripts de prueba, procedimientos de prueba y resultados esperados de las pruebas. El propósito de las pruebas de seguridad de sistemas es examinar la efectividad de los controles de seguridad de un sistema de TI que han sido aplicados en su ambiente operacional. Tienen como objetivo asegurarse de que los controles aplicados cumplen con las especificaciones de seguridad del software y hardware, y que se cubren las políticas de seguridad de la organización o estándares de la industria.

  Pruebas de penetración pueden ser utilizadas como complemento para revisar los controles de seguridad. Cuando se utiliza en el proceso de evaluación de riesgos, sirve para valorar la habilidad del sistema de TI para resistir intentos intencionales de eludir la seguridad de éste. Su objetivo es examinar al sistema desde el punto de vista de la amenaza e identificar fallas potenciales en su esquema de seguridad.

- El desarrollo de una lista de verificación de requerimientos de seguridad, listando los que se encuentren estipulados para el sistema de TI analizado que fueron recolectados durante el paso de caracterización del sistema, para asegurarse de que éstos son cumplidos por controles existentes o planeados. Comúnmente, dicha lista es presentada en forma de tabla, con cada requerimiento acompañado por una explicación de cómo se satisface o no el requerimiento de seguridad.

Dicha lista de verificación contiene los elementos básicos de seguridad que pueden ser utilizados para la evaluación e identificación de vulnerabilidades en los activos (personal, hardware, software e información), procedimientos no automatizados, procesos y transferencias de información asociadas a un sistema de TI en las siguientes áreas de seguridad: gestión, operacional y técnica.

Los tipos de vulnerabilidades que puedan existir, y la metodología requerida para determinarlas, por lo regular varía dependiendo de la naturaleza del Sistema de TI que se esté analizando y la fase en que se encuentre, por ejemplo:

- *Si el sistema de TI aún no ha sido diseñado*, la búsqueda de vulnerabilidades deberá de estar enfocada en las políticas de seguridad de la organización, procedimientos de seguridad planeados y la definición de requerimientos de seguridad. También deberá de tomarse en cuenta los análisis de seguridad que ofrecen los proveedores o desarrolladores de productos de seguridad, como por ejemplo RFC´s.
- *Si el sistema de TI se está desarrollando*, la identificación de vulnerabilidades deberá de incluir información más específica, como las características de seguridad descritas en la documentación del diseño del Sistema y los resultados de evaluaciones y auditorias que se hayan aplicado.
- *Si el sistema de TI se encuentra en operación*, el proceso de identificar vulnerabilidades deberá de incluir el análisis de las características de seguridad y de los controles de seguridad, técnicos y no técnicos, utilizados en el sistema.

Se pueden identificar vulnerabilidades técnicas y no técnicas asociadas al sistema de TI, por medio de las técnicas de recolección de información descritas durante la caracterización del sistema (elaboración de cuestionarios, revisión de documentación, entrevistas en el sitio y utilización de herramientas de escaneo automático)

El Internet es otra gran fuente de información de vulnerabilidades conocidas que se han publicado por los proveedores, o investigadores de seguridad, así como con parches de seguridad, service packs y otras medidas que pueden ser aplicadas para eliminar o mitigar ciertas vulnerabilidades. Algunas fuentes de información de vulnerabilidades que deberán de ser consideradas en un análisis profundo de vulnerabilidades incluyen (entre otras):

- Documentación de Gestión de Riesgos realizada previamente al sistema.

- Reportes de auditorías, anomalías, revisiones de seguridad, de pruebas y evaluaciones al Sistema.
- Equipos de respuesta a incidentes informáticos y listas de correo, por ejemplo en SecurityFocus.com
- Análisis de seguridad aplicadas a software

Para una identificación eficaz de vulnerabilidades del sistema, pueden utilizarse también herramientas de escaneo automático de vulnerabilidades, pruebas y evaluaciones de seguridad y pruebas de penetración.

Las herramientas de escaneo automático de vulnerabilidades son utilizadas para el escanear un grupo de hosts o un segmento de red, buscando servicios vulnerables conocidos, como por ejemplo Microsoft IIS (Microsoft Internet Information Server), FTP anónimo, o telnet. Sin embargo, debe tenerse en cuenta que algunas de las vulnerabilidades potenciales que pueden ser identificadas por este tipo de herramientas, pueden no ser vulnerabilidades reales, es decir, pueden no ser vulnerabilidades que afecten el correcto funcionamiento de algunos sistemas en determinadas situaciones. Por lo que dichas herramientas pueden producir falsos positivos.

La tabla siguiente muestra criterios sugeridos para la identificación de vulnerabilidades de seguridad por cada área:

Área de Seguridad	Criterios de Seguridad
Gestión de Seguridad	- Asignación de responsabilidades - Continuidad de soporte - Capacidad de respuesta a incidentes - Revisiones periódicas de controles de seguridad - Liquidación de personal - Evaluación de riesgos - Entrenamiento de seguridad a personal - Separación de deberes - Autorizaciones en el sistema
Seguridad Operacional	- Control de contaminantes (humo, polvo, químicos) - Controles para asegurar el suministro de energía eléctrica - Acceso y eliminación a medios de almacenamiento - Protección de infraestructura (áreas de cómputo, data centres, oficinas) - Controles de humedad - Controles de temperatura - Laptops y PC´s
Seguridad Técnica	- Comunicaciones (interconexión, ruteadores, switches) - Criptografía - Control de Acceso Discrecional (DAC) - Identificación y autenticación - Detección de Intrusos - Reutilización de objetos - Auditorias al Sistema

Tabla 2.6 Criterios de Seguridad

En el NIST SP 800-26 (*Security Self-Assessment Guide for Information Technology Systems*), se da un cuestionario muestra que contiene objetivos de control específicos que un sistema o grupo de sistemas interconectados que pueden ser valorados y medidos.

- *Resultados obtenidos de la Identificación de Vulnerabilidades:* La lista de las vulnerabilidades que pueden ser explotadas amenazas potenciales.

- ***Paso 4. ANÁLISIS DE CONTROLES***

  En este paso se analizarán los controles implantados por la organización, o en proceso de implantarse para minimizar o eliminar la probabilidad de una amenaza de explotar una vulnerabilidad.

  Una vulnerabilidad tiene una probabilidad baja de ser aprovechada si existe un interés bajo por parte de la amenaza o si ésta tiene capacidades muy limitadas, o bien, si existen controles de seguridad que son efectivos que puedan eliminar o reducir la magnitud del daño que podrían causar.

  Los controles de seguridad pueden ser tanto métodos técnicos, como no técnicos (administrativos, legales o físicos). Los controles técnicos son defensas o protecciones que son incorporados al hardware, software o firmware, como por ejemplo mecanismos de control de acceso, mecanismos de identificación y autenticación, métodos de cifrado, software de detección de intrusos, entre otros. Los controles no técnicos son controles operacionales y de gestión, como por ejemplo políticas de seguridad, procedimientos operacionales, mecanismos de seguridad física y del personal.

  Dichos controles pueden ser clasificados como preventivos o de detección:

- *Controles preventivos*. Disminuyen la ocurrencia de eventos que puedan llegar a afectar al Sistema. En este tipo de controles se encuentran mecanismos como el cifrado, control de acceso, políticas de seguridad y autenticación.
- *Controles de detección.* Ayudan al descubrimiento o intento de violaciones. Como ejemplos de dichos controles se tienen auditorias, métodos de detección de intrusos, métodos de prevención contra intrusos, funciones hash, software de detección de código malicioso, entre otros.

  La implantación de los controles en fases posteriores es el resultado de la identificación de las deficiencias de estos, como por ejemplo que no se encuentren correctamente manejados o que no se hayan colocado debidamente en la infraestructura de la organización.

  Pueden analizarse los controles de seguridad, mediante el desarrollo de listas de verificación o el uso de listas existentes para poderse realizar de manera eficiente y

sistemática. Estas listas pueden ser utilizadas para la validación de cumplimientos o incumplimientos de medidas de seguridad; deberán de ser actualizadas periódicamente para que, en caso de que se den cambios en la organización, se vean reflejados en ellas, para que puedan ser tomadas como válidas.

- *Resultados obtenidos del Análisis de Controles:* Una lista de los controles utilizados o planeados a implantar en el sistema de TI, utilizados para mitigar la probabilidad de que una vulnerabilidad sea explotada, y reduzca el impacto en caso de que se dé un incidente de seguridad

- ***Paso 5. DETERMINACIÓN DE PROBABILIDAD DE OCURRENCIA***

Para la obtención de un índice de probabilidad cualitativo que sea útil en la medición de la probabilidad, se deben de tomar en consideración factores como la motivación y capacidades de la amenaza, el tipo de la vulnerabilidad y la existencia y efectividad de controles de seguridad implantados.

Dicho índice de probabilidad puede ser descrito como sigue:

- **Alto**. La amenaza está altamente motivada, es suficientemente capaz y los controles colocados para prevenir que se explote la vulnerabilidad no son efectivos.
- **Medio**. La amenaza se encuentra motivada y capacitada, pero existen controles colocados para impedir la exitosa explotación de la vulnerabilidad.
- **Bajo**. La amenaza carece de motivación o capacidad, o se encuentran controles correctamente colocados que impiden o al menos previenen que la vulnerabilidad pueda ser aprovechada.

- *Resultados obtenidos de la Determinación de probabilidad de ocurrencia:* Índice de probabilidad de explotación de vulnerabilidades.

- ***Paso 6. ANÁLISIS DE IMPACTO***

  En este punto, se medirá el impacto adverso a la organización, del resultado la explotación exitosa de una vulnerabilidad.

  Se deberá tener en cuenta la información recabada previamente, como la misión, nivel crítico y sensitividad (tanto de la información, como del sistema).

  Se puede tomar como punto de partida la información existente en documentos de la organización como reportes de análisis de impacto o reportes de evaluación del de activos.

  Un reporte de análisis de impacto, también conocido como *Análisis de Impacto del Negocio (BIA, Business Impact Analysis)*, asigna prioridades a los niveles de impacto asociado a la afectación de los activos de la organización, basándose en evaluaciones cualitativas o cuantitativas del nivel crítico y sensitividad de dichos activos.

  Un reporte de evaluación del de activos, identifica y asigna prioridades a los activos que manejan información crítica y sensible de la organización que fundamentan la misión de la organización.

  La sensibilidad de un sistema o información puede determinarse por el nivel de protección requerida para mantener la confidencialidad, integridad y disponibilidad del sistema.

  Sin importar el método con el que se determine la sensibilidad de un sistema de TI y la información que maneja, los dueños de éstos son los últimos responsables en la asignación del grado asignado para sus propios sistemas e información. Por lo que en el análisis del impacto, se deberá de entrevistarlos, porque al final, su punto de vista será el que tenga mayor peso.

  Entonces, el impacto adverso que un incidente de seguridad puede ocasionar, puede ser descrito en términos de la pérdida, degradación o combinación de ambos, de tres servicios de seguridad: confidencialidad, integridad y disponibilidad. A continuación se describe el impacto general de que dichos servicios no sean cumplidos.

- **Pérdida de Confidencialidad**. El impacto de la pérdida de éste servicio de seguridad, puede resultar en divulgación de información clasificada, uso no autorizado de dicha información, que podría ser utilizada para fines no autorizados.
- **Pérdida de Integridad**. Si ésta no es corregida oportunamente, el uso continuo de la información corrupta o contaminada, puede resultar en inexactitudes, fraudes o tomas de decisiones erróneas. Hay que tomar en cuenta, de que las violaciones de integridad, usualmente son el primer paso de ataques a la confidencialidad o disponibilidad de sistemas.
- **Pérdida de Disponibilidad**. Si un sistema de TI crítico no se encontrara disponible para los usuarios finales, la misión de la organización puede verse afectada. Por ejemplo, la pérdida de funcionalidad de un sistema o su efectividad operacional, puede resultar en pérdidas de tiempo productivo, reduciendo así el rendimiento de los usuarios finales en sus asignaciones que apoyan la misión de la organización

  En algunos casos, el impacto puede ser medido cuantitativamente, como por ejemplo en pérdida de ingresos, costos de reparación, el nivel de esfuerzo requerido por el personal para corregir los problemas causados por ataques exitosos. También existen casos donde el impacto no puede ser descrito en números pero se les puede asignar un grado, ya sea alto, medio o bajo, como por ejemplo la pérdida de la confianza pública, pérdida de credibilidad o daños a los intereses de la organización.

Se puede definir el grado del impacto a la organización de acuerdo a la siguiente tabla:

Magnitud del Impacto	Definición
Alto	El ejercicio de la vulnerabilidad puede: - Resultar en pérdidas altamente costosas de activos tangibles o recursos - Violar, dañar o impedir significativamente la misión de la organización - Resultar en muerte o lesiones graves
Medio	El ejercicio de la vulnerabilidad puede: - Resultar en pérdidas costosas de activos tangibles o recursos - Violar, dañar o impedir la misión de la organización - Resultar en lesiones
Bajo	El ejercicio de la vulnerabilidad puede: - Resultar en pérdidas de activos tangibles o recursos - Afectar notablemente la misión de la organización

Tabla 2.7 Magnitud del impacto ocasionado a la organización

- *Resultados obtenidos del Análisis de Impacto:* Magnitud de Impacto (Alto, Medio o Bajo).

- ***Paso 7. DETERMINACIÓN DEL RIESGO***

Es en este paso donde realmente se lleva la evaluación de los riesgos en un sistema de TI. La determinación del riesgo para un par amenaza/vulnerabilidad en particular puede ser expresada en función de:

- La probabilidad de ocurrencia de que una amenaza dada, explote una cierta vulnerabilidad.
- La magnitud del impacto ocasionado a la organización cuando la amenaza aproveche exitosamente la vulnerabilidad.
- La medida en que controles de seguridad existentes o planeados reducen o eliminan el riesgo.

En la medición del riesgo, se deberá de desarrollar una escala y una matriz de nivel de riesgo. Para la obtención de grados en la escala de riesgos, se debe de multiplicar los valores que se han asignado a la probabilidad de ocurrencia y al impacto que podría ocasionarse. La siguiente matriz de 3X3 muestra cómo se obtendrá dicho valor, aunque en ocasiones dicha matriz podría variar en sus dimensiones, es decir, podría ser de 4X4 en caso de tener valores de probabilidad y de impacto de *muy alto*, por ejemplo en caso de requerir el apagado de un equipo, o de *muy bajo*.

PROBABILIDAD de Ocurrencia	**IMPACTO**		
	***Bajo** (10)*	***Medio** (50)*	***Alto** (100)*
***Alto** (1.0)*	**Bajo** 10 X 1.0 = 10	**Medio** 50 X 1.0 = 50	**Alto** 100 X 1.0 = 100
***Medio** (0.5)*	**Bajo** 10 X 0.5 = 5	**Medio** 50 X 0.5 = 25	**Medio** 100 X 0.5 = 50
***Bajo** (0.1)*	**Bajo** 10 X 0.1 = 1	**Bajo** 50 X 0.1 = 5	**Bajo** 100 X 0.1 = 10

Tabla 2.8 Magnitud del impacto ocasionado a la organización

A partir de los valores obtenidos de la matriz anterior, se deberán de tomar acciones que los dueños de la información deberán de realizar:

- **Riesgo Alto**. Existe una alta necesidad de realizar medidas correctivas. Un sistema puede continuar en operación, pero se deberá de implantar un plan de acciones correctivas lo más rápido posible.
- **Riesgo Medio**. Existe una necesidad de realizar medidas correctivas y se deberá de desarrollar un plan que incorpore dichas medidas en un periodo de tiempo razonable.
- **Riesgo Bajo**. Una autoridad designada deberá de determinar si acciones correctivas son requeridas o si se decide la aceptación de dicho riesgo.

- *Resultados obtenidos de la Determinación del Riesgo:* Magnitud de Riesgo (Alto, Medio o Bajo).

- ***Paso 8. RECOMENDACIÓN DE CONTROLES***

  En esta etapa, se proveen los controles que podrían mitigar o eliminar los riesgos identificados de acuerdo a la organización. El objetivo de la recomendación de controles es la reducción de los niveles de riesgo a un sistema de TI y su información a niveles aceptables.

  Se deberán de tomar en consideración factores para la recomendación de controles y soluciones alternativas para minimizar o eliminar los riesgos identificados, por ejemplo:

- La efectividad de las opciones recomendadas en el entorno de la organización
- Regulaciones y legislaciones a las que se encuentra sujeto el sistema
- Políticas de la organización
- Impacto operacional
- Confianza

Los controles recomendados son el resultado de la evaluación de riesgos y son el punto de partida para el proceso de mitigación de riesgos. En dicho proceso los controles de seguridad técnicos y de procedimiento son evaluados, categorizados e implantados.

■ *Resultados obtenidos de la Recomendación de Controles:* Listado de controles (técnicos y operacionales) de seguridad para mitigar el valor de riesgos.

- ***Paso 9. DOCUMENTACIÓN DE RESULTADOS***

  Al finalizar el proceso de *evaluación de riesgos* (amenaza y vulnerabilidades identificadas, riesgos determinados y controles de seguridad recomendados), los resultados deberán de ser documentados en un reporte.

  Un reporte de evaluación de riesgos ayuda a los dueños de la información, a realizar decisiones en políticas, de procedimiento, presupuestales, operacionales y cambios gerenciales. A diferencia de otro tipo de reportes, como de auditorías o de investigación que se enfocan en la búsqueda de infractores, un reporte de evaluación de riesgos no deberá de ser presentado en un estilo denunciante, más bien se deberá tener un acercamiento sistemático y analítico de la evaluación de riesgos para que la alta gerencia logre entender los riesgos y asigne recursos para la reducción o pérdida eventual de dichos riesgos.

  - *Resultados obtenidos de la Documentación de Resultados:* Reporte de evaluación de riesgos, donde se describen las amenazas y vulnerabilidades, se miden los riesgos y se aportan recomendaciones de controles de seguridad.

MITIGACIÓN DE RIESGOS

La mitigación de riesgos es el segundo proceso en la *gestión de riesgos*, es donde se priorizan, evalúan e implantan los controles recomendados resultado del proceso de evaluación de riesgos.

La eliminación de un riesgo resulta sumamente difícil, o considerarse prácticamente imposible, por esto se deberá de tener un acercamiento del menor costo e implantar los controles más apropiados para decrecer el riesgo hasta niveles aceptables, realizando un impacto adverso mínimo en la misión y recursos de la organización.

La *mitigación de riesgos* se podrá alcanzar mediante sólo una de las siguientes opciones:

- **Aceptación del Riesgo**. Se acepta el riesgo potencial y el sistema de TI continúa en operación o se implantan controles para la reducción del riesgo a un nivel aceptable.
- **Evitar el Riesgo**. Se evita el riesgo eliminando la causa y/o la consecuencia.
- **Limitación del Riesgo**. Se limita el riesgo implantando controles que minimizan el impacto adverso de la explotación de una vulnerabilidad.
- **Planeación del Riesgo**. Se administran los riesgos desarrollando un plan de mitigación de riesgos que prioriza, implanta y mantiene controles de seguridad.
- **Investigación y Reconocimiento**. Se reduce el riesgo reconociendo la vulnerabilidad o falla e investigando qué controles pueden corregirla.
- **Transferencia del Riesgo**. Se transfiere el riesgo, utilizando distintas opciones para la compensación de pérdidas, por ejemplo la adquisición de un seguro.

Para escoger cualquiera de estas opciones, se deberá de tomar en cuenta los objetivos de la misión de la organización. Puede resultar impráctico en algunas ocasiones la implantación de algún control en todos los riesgos identificados, por lo que se deben de asignar prioridades a los pares amenaza/vulnerabilidad que tienen un potencial de causar mayor daño a la misión. Los controles variarán dependiendo el entorno de la organización.

Para ayudar en la toma de decisión de implantar o no un control de seguridad, se cuenta con la estrategia de mitigación de riesgo mostrada en la Figura 3.4

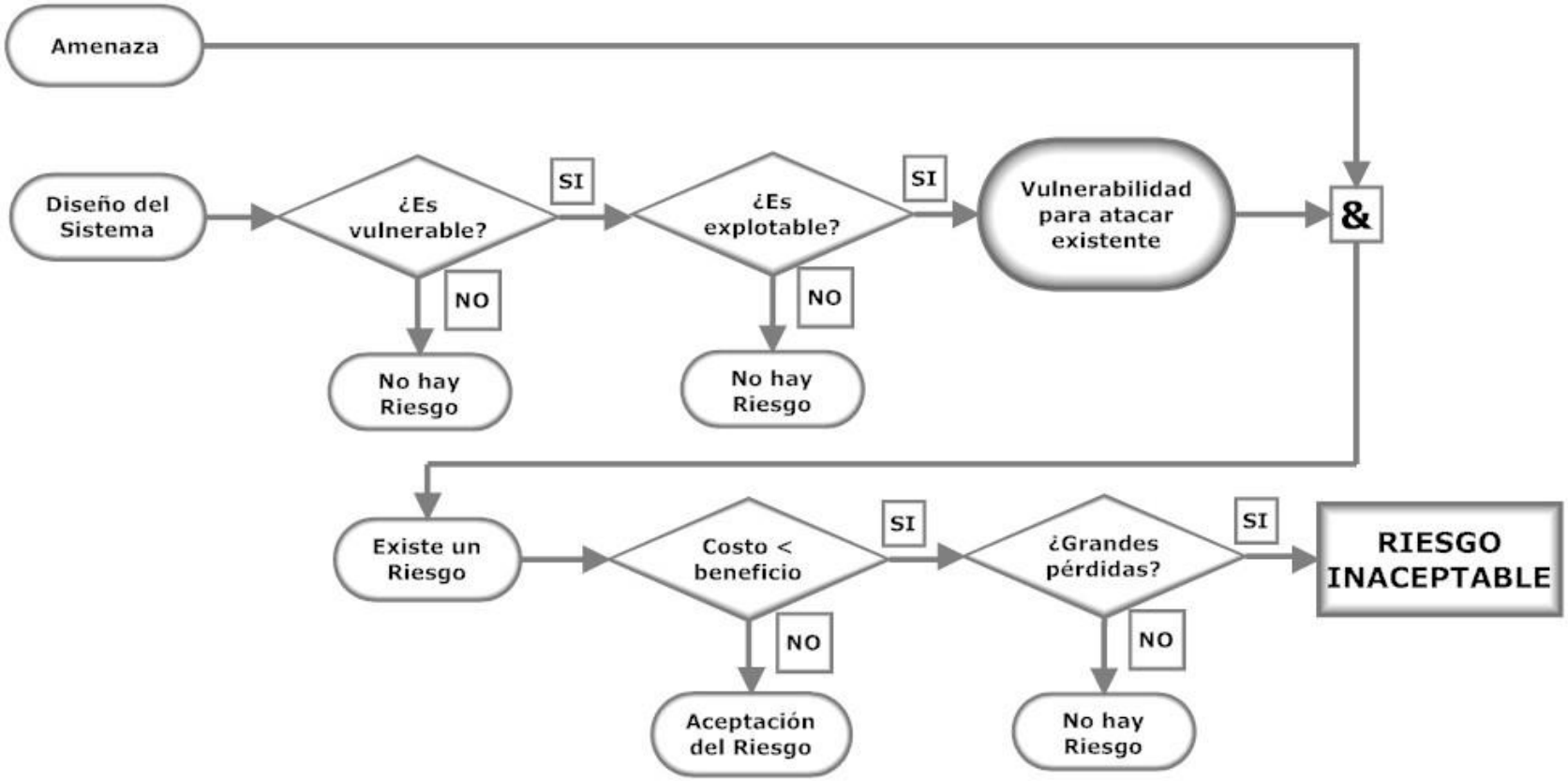


Figura 2.9 Estrategia de mitigación de riesgo

En dicha estrategia, donde se indique la respuesta "SI", se deberán de tomar las acciones siguientes:

- **Cuando existe una vulnerabilidad**. Implantar técnicas que garanticen la reducción de la probabilidad de ocurrencia de que ésta sea explotada
- **Cuando una vulnerabilidad puede ser explotada**. Se aplican protecciones o controles administrativos que minimicen el riesgo o prevenga su ocurrencia.
- **Cuando el costo del atacante es menor que el beneficio que podría obtener**. Se aplican protecciones que hagan disminuir la motivación del atacante, incrementando el costo que supondría aplicar la explotación de la vulnerabilidad.
- **Cuando la pérdida es muy grande**. Se aplican cambios al diseño y arquitectura, se implantan protecciones técnicas y no técnicas que limiten la extensión del ataque, reduciendo las pérdidas potenciales.

La estrategia anterior puede aplicarse también cuando los riesgos son derivados de amenazas ambientales o humanas no intencionales. Debido a que no existe la figura del atacante en dichas amenazas.

En los casos de que se deban de realizar acciones, se deberá de seguir la siguiente regla: *Enfocarse en los riesgos mayores y realizar los esfuerzos necesarios de mitigación de riesgos al menor costo, causando un impacto mínimo en la misión de la organización*.

En la Figura 2.10 se describen los pasos de la *mitigación de riesgos*

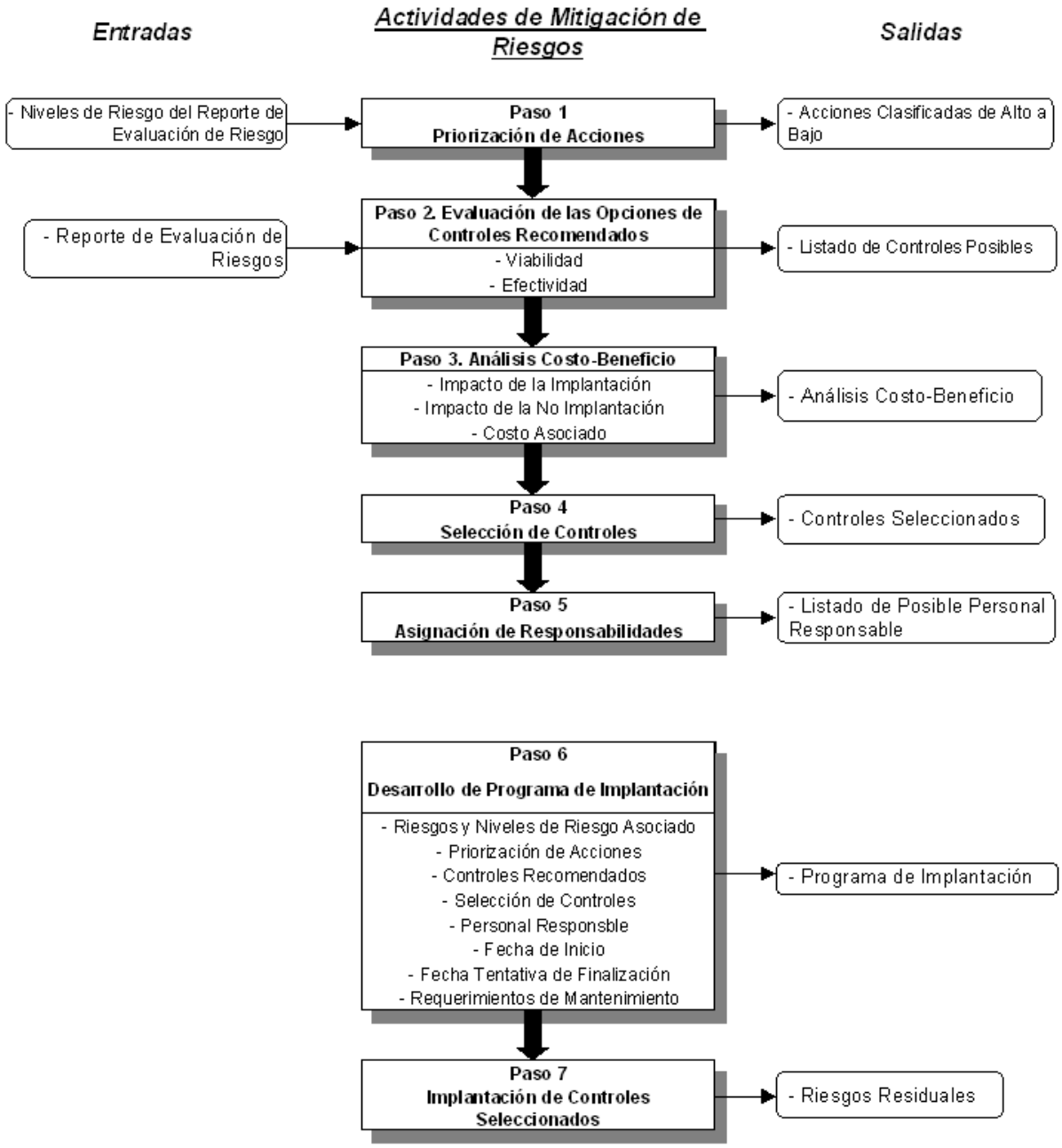


Figura 2.10 Actividades de mitigación de riesgos

- ***Paso 1. PRIORIZACIÓN DE ACCIONES.***

Basándose en los niveles de riesgo obtenidos del reporte de evaluación de riesgos, las acciones de implantación serán catalogadas. Para la reservación de recursos, la mayor prioridad se asignará a los niveles de riesgo que sean inaceptablemente altos. Dichos pares amenaza/vulnerabilidad requerirán de acciones correctivas inmediatas para proteger la misión de la organización.

Nivel de Acción	Definición
Alta	Es necesaria y urgente su aplicación
Media	Es necesaria su aplicación
Baja	No es muy necesaria su aplicación

Tabla 3.6 Niveles de prioridad de acciones

- *Resultados obtenidos de la Priorización de Acciones:* Niveles (Alta, Media y Baja) de prioridad asociados a las acciones a tomar.

- ***Paso 2. EVALUACIÓN DE LAS OPCIONES DE CONTROLES RECOMENDADOS***

Los controles recomendados en el reporte de evaluación de riesgos pueden no ser los más apropiados para algunas organizaciones en específico. Por lo que se debe de analizar la fiabilidad (por ejemplo, compatibilidad y aceptación de los usuarios) y efectividad (por ejemplo, el grado de protección y nivel de mitigación del riesgo) de las opciones de controles recomendadas. El objetivo final será la selección de los controles de seguridad más apropiados para mitigar los riesgos.

- *Resultados obtenidos de la Evaluación de las Opciones de Controles Recomendados:* Lista de controles posibles.

- **Análisis Costo-Beneficio**

Después de la identificación de los posibles controles y la evaluación de fiabilidad y efectividad de éstos, se deberá de realizar un análisis costo-beneficio a cada control propuesto, para lograr determinar cuáles son los controles requeridos y apropiados para la organización.

Dicho análisis puede realizarse de manera cualitativa o cuantitativa. Ya que tiene como propósito demostrar que el costo de la implantación del control es justificable por la reducción del riesgo asociado.

El análisis abarca lo siguiente:

- Determinación del impacto de la implantación de un nuevo control o el reforzamiento de uno existente
- Determinación del impacto de la NO implantación de un nuevo control o el reforzamiento de uno existente
- Estimación de los costos de implantación. Se pueden tener en consideración:

  - Adquisición de hardware y software
  - Reducción de efectividad operacional si el rendimiento o funcionalidad del sistema es reducido para aumentar la seguridad
  - Costo de la implantación de políticas y procedimientos adicionales
  - Costo de contratación de personal adicional para la implantación de políticas, procedimientos o servicios.
  - Costos de entrenamiento de personal
  - Costos de mantenimiento

- *Resultados obtenidos del Análisis Costo-Beneficio:* Descripción del costo y el beneficio de la implantación y la no implantación de controles de seguridad.

- **Selección de Controles**

En la implantación de los controles recomendados, se deben de considerar controles de seguridad técnicos, administrativos, operacionales o combinaciones de éstos, para lograr una prevención, limitación o deterioro del daño que causaría la amenaza.

Con base en el análisis costo-beneficio, la administración determinará los controles que convienen más a la organización, para la reducción de los riesgos.

- *Resultados obtenidos de la Selección de Controles*: Listado de los controles seleccionados.

- **Asignación de Responsabilidades**

Se identifica y responsabiliza al personal adecuado que tenga la experiencia apropiada y las habilidades necesarias para implantar los controles seleccionados.

- *Resultados obtenidos de Asignación de Responsabilidades*: Listado del personal responsable.

- **Desarrollo del Programa de Implantación**

En este paso se desarrollará un programa que garantice la implantación de los controles. Deberá de contener:

— Riesgos (pares amenaza/vulnerabilidad) y niveles de riesgo asociados, obtenidos del reporte de evaluación de riesgos
— Controles recomendados obtenidos del reporte de evaluación de riesgos
— Prioridad de las acciones
— Selección de los controles programados a implantar, en base a la fiabilidad, efectividad, beneficios y costo

- Listado de personal responsable
- Fecha de inicio de la implantación
- Fecha tentativa de terminación de la implantación
- Requerimientos de mantenimiento

■ *Resultados obtenidos del Desarrollo del Programa de Implantación:* Programa de Implantación de controles.

- **Implantación de los Controles Seleccionados y Análisis de Riesgos Residuales**

En la mayoría de los casos, los controles implantados podrán reducir el nivel del riesgo, pero no eliminarlo por completo.

La dirección de la organización deberá determinar lo que es un nivel aceptable de riesgo. Se evalúa el impacto del riesgo según lo siguiente:

- Si el control de seguridad reduciría el riesgo mucho más de lo necesario, entonces se deberá de buscar una alternativa menos costosa.
- Si un control costaría más que lo que costaría la reducción del riesgo, entonces se deberá de buscar otra opción.
- Si un control no reduce lo suficiente el riesgo, entonces se deberá de buscar la implantación de varios controles a la vez o de otro tipo de controles.
- Si un control suministra una reducción suficiente de riesgo y es viable económicamente, entonces se procede a su utilización.

Con frecuencia, el costo de la implantación de un control es más fácil de identificar, que el costo de la no implantación. Por esto, la gerencia de la organización juega un papel fundamental en la toma de decisiones que conciernen a la implantación de controles de seguridad que protegerán la misión.

Las organizaciones pueden analizar la reducción de los riesgos generada por la implantación de nuevos controles o el reforzamiento de los ya establecidos, en términos del decrecimiento de la probabilidad de ocurrencia o del impacto, que son los dos parámetros que definen el nivel del riesgo.

La implantación de nuevos controles o el reforzamiento de los ya existentes, pueden mitigar el riesgo por las siguientes maneras:

- La eliminación de algunas de las vulnerabilidades del sistema, por lo que se reduce el número posible de pares amenaza/vulnerabilidad
- La agregación de controles dirigidos que reduzcan la capacidad y motivación de la amenaza
- La reducción de la magnitud del impacto adverso.

El riesgo remanente después de la implantación de nuevos controles o el reforzamiento de controles previos es el *riesgo residual.*

En la figura 2.11, se muestra la relación entre la implantación de controles y el riesgo residual:

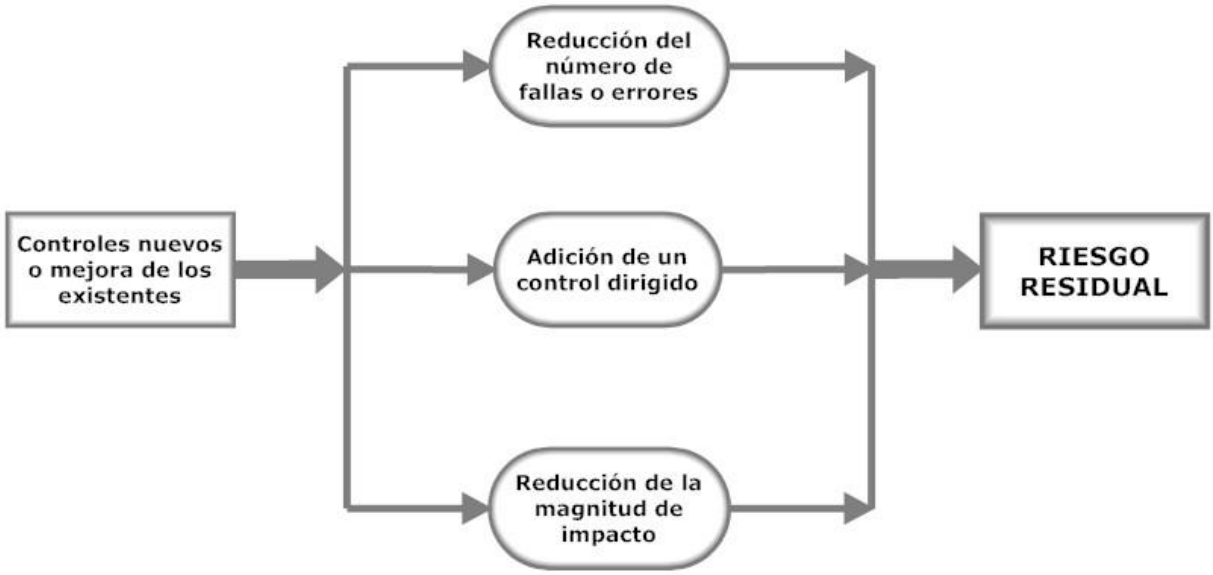


Figura 2.11 Implantación de controles y riesgo residual

Prácticamente no existe sistema de TI alguno que se encuentre libre de riesgos, y no todos los controles que se implanten pueden eliminar el riesgo por completo.

La autoridad autorizadora aprobada será la responsable de la aprobación de la aceptación de los riesgos residuales por escrito para que continúe en operación el sistema de TI. Si el riesgo residual no ha sido reducido a un nivel aceptable, el ciclo de gestión de riesgos

deberá de repetirse para poder identificar una alternativa que lo disminuya a niveles aceptables.

- *Resultados obtenidos la Implantación de los Controles Seleccionados y el Análisis de Riesgos Residuales:* Reporte de avances y/o terminación de la implantación de controles de seguridad. Así como los riesgos residuales aceptados.

- **GESTIÓN Y EVALUACIÓN**

En la mayoría de las organizaciones, la red de datos estará en continua expansión y actualización se realizarán cambios en sus componentes y el software aplicativo será reemplazado o actualizado con versiones más nuevas. Además el personal y las políticas de seguridad son propensas a ir cambiando en el tiempo. Por todo esto, riesgos nuevos surgirán y los riesgos que se han mitigado anteriormente pueden volver a ser una preocupación. Entonces, la gestión de riesgos es un proceso continuo y demandante.

En los Estados Unidos, por mandato presidencial (OMB Circular A-130 de la Casa Blanca) el proceso de evaluación de riesgos se debe repetir al menos cada 3 años para agencias federales, en nuestro país no hay regulación alguna al respecto. Sin embargo, dicho proceso debe ser realizado no porque sea obligatorio por alguna ley o regulación, sino porque es una buena práctica y apoya a los objetivos de la misión de la organización. Se deberá llevar entonces un proceso de gestión de riesgos de manera periódica, pero de manera suficientemente flexible para permitir cambios donde se justifiquen, como por ejemplo cambios mayores al sistema de TI y su ambiente operacional debido a cambios de políticas de la organización o a nuevas tecnologías.

Las claves para una gestión de riesgos exitosa son:

- Compromiso de la alta gerencia
- Apoyo total y participación del personal de TI
- La eficiencia del personal de la evaluación de riesgos
- La conciencia y cooperación de los miembros de la comunidad de los usuarios del sistema de TI, que deberán seguir procedimientos y cumplir con los controles implantados para garantizar el cumplimiento de la misión de la organización

Una evaluación continua de los riesgos relacionados

2.2 ISO 27002:2005

La serie ISO/IEC 27000 es un conjunto de estándares de seguridad desarrollados por la International Organization for Standars (ISO) y la International Electrotechnical Comisión (IEC) derivados del estándar británico BS 7799.

Los estándares publicados de la serie 27000 son los siguientes:

- *ISO27000*. Introducción y glosario.
- *ISO 27001*. Requerimientos para un Sistema de Gestión de Seguridad de la Información (SGSI).
- *ISO 27002*. Controles de seguridad para un SGSI.
- *ISO 27005*. Gestión de Riesgos para un SGSI.
- *ISO 27006*. Guía para la certificación de un SGSI.
- *ISO 27011*. SGSI para industrias de telecomunicaciones.

La siguiente figura muestra cómo ha sido la evolución a través del tiempo de los estándares ISO 27001 y 27002:

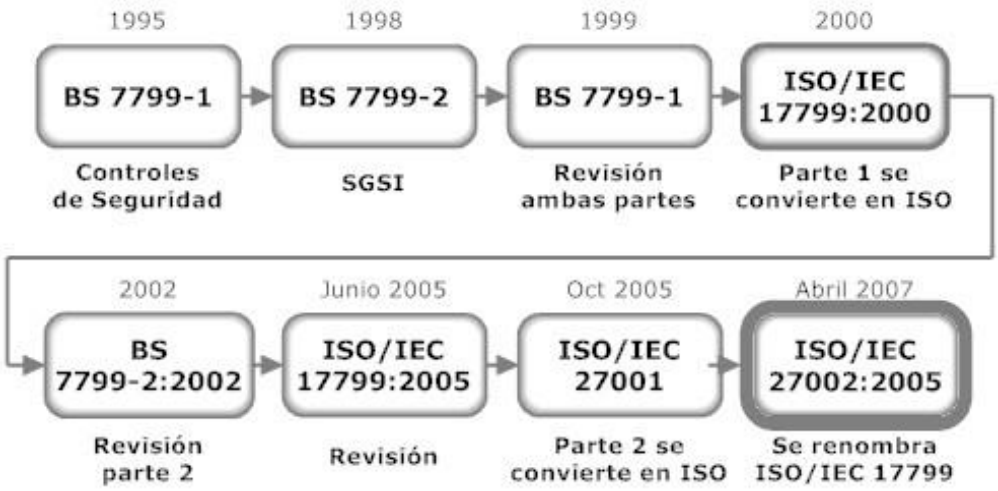


Figura 2.12 Cronología ISO 27001 e ISO 27002

ISO 27002. Incluye 11 cláusulas de control de seguridad, con un total de 39 categorías de seguridad principales, en total son 133 controles de seguridad diseñados para ser implantados y que satisfagan los requerimientos de seguridad identificados por una gestión de riesgos.

Cada categoría de seguridad incluye un objetivo de control y uno o varios controles aplicables para lograrlo. Las cláusulas definidas en el estándar son las siguientes:

Política de Seguridad (1 categoría, 2 controles). Brinda un lineamiento de implementación del documento de la política de seguridad, así como la revisión del mismo.

Organización de la Seguridad de la Información (2 categorías, 11 controles). Fija un marco referencial para el manejo de la seguridad, tanto una organización interna, como hacia terceros.

Gestión de Activos (2 categorías, 5 controles). Establece responsabilidades sobre los activos, así como su clasificación.

Seguridad de Recursos Humanos (3 categorías, 9 controles). Brinda una serie de controles a implantar antes, durante y en el cese o cambio de personal.

Seguridad Física y Ambiental (2 categorías, 13 controles). Indica medidas para establecer áreas seguras y la protección de equipo.

Gestión de Comunicaciones y Operaciones (10 categorías, 32 controles). Garantiza una apropiada operación de los medios de procesamiento de la información, como protección contra código malicioso, copias de seguridad, seguridad en redes, entre otros.

Control de Acceso (7 categorías, 25 controles). Gestiona el control de acceso tanto de usuarios, a la red, al sistema operativo, aplicaciones y equipo fuera de sitio.

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6 categorías, 16 controles). Brinda los requisitos de seguridad necesarios para los sistemas de información.

Gestión de Incidentes de Seguridad de la Información (2 categorías, 5 controles). Indica controles a implantar en el caso de eventos relacionados con la seguridad.

Gestión de la Continuidad del Negocio (1 categoría, 5 controles). Establece controles a aplicar en caso de una suspensión de las actividades comerciales, así como su protección. También brinda lineamientos para la implementación de planes de continuidad.

Conformidad (3 categorías de seguridad, 10 controles). Para el cumplimiento de requerimientos legales, de políticas y normas. También establece ciertas consideraciones para realizar auditorías a los sistemas de información.

CAPÍTULO 3. ANÁLISIS Y PLANTEAMIENTO DE LA PROPUESTA

En este capítulo se realiza la gestión de riesgo basada en la metodología basada en la Figura 3.1 y como producto final se plantea un programa de implantación de los distintos controles de seguridad seleccionados.

La información manejada tiene como fecha de corte de adquisición el mes de Septiembre de 2009.

3.1 Análisis de Riesgo

A continuación se describen las actividades requeridas en el proceso de Análisis de Riesgos. (Ver Figura 3.3):

1. Caracterización del Sistema.
2. Identificación de Amenazas.
3. Identificación de Vulnerabilidades.
4. Análisis de Controles.
5. Determinación de la Probabilidad de Ocurrencia.
6. Análisis de Impacto.
7. Determinación del Riesgo.
8. Recomendación de Controles.
9. Documentación de Resultados.

3.1.1 Caracterización del Sistema

- **Hardware**

- Aproximadamente 350 equipos de cómputo (PC´s y laptops). Del cual aproximadamente una cuarta parte cuenta con procesadores obsoletos como Pentium Celeron, Pentium II, Pentium III y anteriores; el equipo restante tiene procesadores Pentium D, Core Duo, Core 2 Duo y equivalentes. La gran mayoría tiene como sistema operativo Windows XP SP3.
- 5 servidores con procesadores de alto rendimiento. Todos corriendo en Linux como sistema operativo
- Alrededor de 50 impresoras, cuyos modelos varían desde los de inyección de tinta, los multifuncionales, hasta los de impresión a grandes volúmenes a color

- Cerca de 30 proyectores
- 19 pizarrones electrónicos
- 17 dispositivos de conexión de redes, entre hubs, switches y access points
- 1 cámara digital
- Alrededor de 135 equipos supresores de picos y no-breaks
- Grán número de memorias USB

- **Software**

- Matemático (Matlab, Matematica, Maple, MathType, Geogebra, Descartes, MathCAD)
- Ofimático (MS Office 2000, 2003 y 2007, OpenOffice)
- Dibujo (AutoCad 2000,2004, 2007, Corel Draw, ChemLab, PSPICE)
- Edición de Archivos (Adobe Acrobat, Photoshop)
- Para lecturas ópticas (Pearson NCS ScanToolsPlus)
- Antivirus (Kaspersky, Avira, McAfee, Norton)
- Estadístico (SPSS, Statistica)
- Bases de Datos (MySQL, PostgreSQL)
- Mensajería (MSN Messenger, Skype)
- Didáctico (Second Life)
- Conectividad (SSH Secure Shell)
- Grabadores de CD y DVD (Nero, Roxio)

- **Tipos de información manejada**

- Académica
- Administrativa
- Administración de redes
- Personal (nombre, dirección, teléfonos, etc...)
- Configuraciones de servicios
- Datos de sesiones de prácticas de laboratorio.

- **Personal que utiliza y mantiene los sistemas de TI**

- Personal de la Coordinación de Cómputo de la DCB

- **Nivel Crítico de los Servidores y Aplicaciones**

Para definir los niveles críticos de los servidores y aplicaciones, se utilizaron los parámetros definidos por Landoll:

- De Misión Crítica: Son aquellos que podrían impedir a la División llevar a cabo su Misión, en caso de alguna falla. Deberá de considerarse un sistema como critico si apoya una función esencial, provee la única fuente de información de datos críticos o puede causar paro inmediato, inclusive la pérdida total.
- Importantes: Son los sistemas cuya falla no imposibilita la realización de la Misión de la División en un corto período, pero que podrían hacerlo, en caso de que no sean reparados a mediano o largo plazo. Se considera importante un sistema si funciona como respaldo de uno que es critic o que podría tener un impacto sustancial, en caso de fallas en un period de tiempo extensor.
- De Apoyo: Son los sistemas cuya falla no evitaría llevar a cabo la Misión de la División, pero que afectaría la efectividad o eficiencia de las operaciones del día a día. Un sistema se considera de apoyo cuando maneja información organizacional o solo causaría pérdidas en caso de fallas al dueño.

- Servidores (por razones de seguridad no se mencionan nombres):
- 5 servidores con nivel crítico Importante
- Aplicaciones (Aplicación – Nivel crítico):
- Sistema Integral de Información de la DCB (SII-DCB) – Importante
- Base de Datos del Sistema Integral de Información de la DCB (SII-DCB) – Importante
- Sistema de gestión de Información del Personal Académico de la DCB (SIGECI-DCB) –De Apoyo
- Sistema de Información de Actividades Académicas de la DCB (SIAA-DCB) – Importante
- Control de Correspondencia –De Apoyo
- Registro de usuarios del TCA – De Apoyo
- Prácticas de Mecánica – De Apoyo

- **Sensibilidad de los Servidores y Aplicaciones**

Para definir los niveles críticos de los servidores y aplicaciones, se utilizaron los parámetros definidos por Landoll:

- Sensibles: Son recursos que contienen cualquier tipo de información sensible, incluyendo información personal de empleados, de configuración de controles de seguridad e información propietaria.
- De Usuario: Recursos que manejan información exclusiva de ciertos usuarios.
- Públicos: Son recursos que no contienen información sensible ni de algún usuario en exclusive.

- Servidores:
  - 2 servidores Sensibles
  - 3 servidores De Usuario
  - En algunos casos los servidores manejan información pública, pero como no se tiene debidamente segregada dicha información, se considerará el nivel se sensibilidad mayor.
- Aplicaciones (Aplicación – Sensibilidad):
  - Sistema Integral de Información de la DCB (SII-DCB) – Sensible
  - Base de Datos del Sistema Integral de Información de la DCB (SII-DCB) – Sensible
  - Sistema de Gestión de Información del Personal Académico de la DCB (SIGECI-DCB) – Sensible
  - Sistema de Información de Actividades Académicas de la DCB (SIAA-DCB) –De Usuario
  - Control de Correspondencia –De Usuario
  - Registro de usuarios del TCA – De Usuario
  - Prácticas de Mecánica – De Usuario

- **Grupos y Usuarios**

- Existe un gran número de grupos en los distintos servidores y aplicaciones de la DCB, van desde grupos de administración, grupos con mínimos privilegios, y grupos con diversos privilegios como de consulta, captura, monitoreo, actualización, entre otros propósitos.

- **Políticas de Seguridad que rigen a la DCB**

- Políticas de Seguridad de la FI
- Políticas de Seguridad de la DCB (en proceso)

- **Topología de la Red**

- El esquema de la red de datos de la DCB se encuentra descrito en el capítulo 2. Se conforma de varias subredes: Laboratorios, Red Local (incluye coordinaciones, secciones académicas, Taller de Cómputo para Académicos y cubículos en general), Taller para la Docencia (incluye los salones del Taller de Cómputo para la Docencia, laptops para préstamo y salones de clase con equipo de cómputo) y Jefatura y Secretaría Académica.

- **Protección de Medios de Almacenamiento de la Información**

- En general, no se cuenta en ningún área con una protección de medios de almacenamiento.

- **Entorno de Seguridad Física de los Sistemas de TI**

- Los equipos cuentan con un resguardo, donde se indica quién es el responsable.
- La gran mayoría sólo se encuentra asegurado de la misma manera que se aseguran los cubículos, únicamente con llave.
- Los equipos ubicados en los salones se encuentran resguardados mediante puertas con cerradura electrónica que hace uso de biometría y control de acceso, además cuentan con alarmas de seguridad.

3.1.2 Identificación de Amenazas

Las amenazas identificadas son las siguientes:

- **Naturales**

- Terremotos

- **Humanas**

- Usuarios no autorizados (personas no pertenecientes a la DCB, alumnos, personas con acceso a la RIU)
- Usuarios autorizados (personal académico-administrativo perteneciente a la DCB)

- **Ambientales**

- Fallas en el suministro de electricidad

3.1.3 Identificación de Vulnerabilidades

Para la identificación de vulnerabilidades potenciales se utilizaron distintas técnicas, como entrevistas a responsables de área, búsqueda de vulnerabilidades publicadas en internet por software comercial, público y gratuito, plataformas y servicios, utilización de herramientas de mapeo de redes, análisis de vulnerabilidades, análisis de vulnerabilidades de sitios web y análisis de vulnerabilidades por parte de terceras personas.

Los cuestionarios utilizados son mostrados en el apartado 6.1 (Documentación de las Actividades de Análisis de Riesgos).

Los sitios utilizados en la búsqueda en internet cuentan con reputación conocida y fiable:

- US-CERT. United States-Computer Emergency Readiness Team (www.kb.cert.org/vuls).
- CVE. Common Vulnerabilities and Exposures (cve.mitre.org).
- NIST-NVD. National Institute of Standards and Technology-National Vulnerability Database (web.nvd.nist.gov).
- SANS Internet Storm Center (isc.sans.org).
- Computer Security Vulnerabilities (securityvulns.com).
- Blogs de seguridad de Microsoft (blogs.technet.com).

Las herramientas de mapeo de redes utilizadas fueron: nmap, 10-Strike Network Inventory y LAN Surveyor

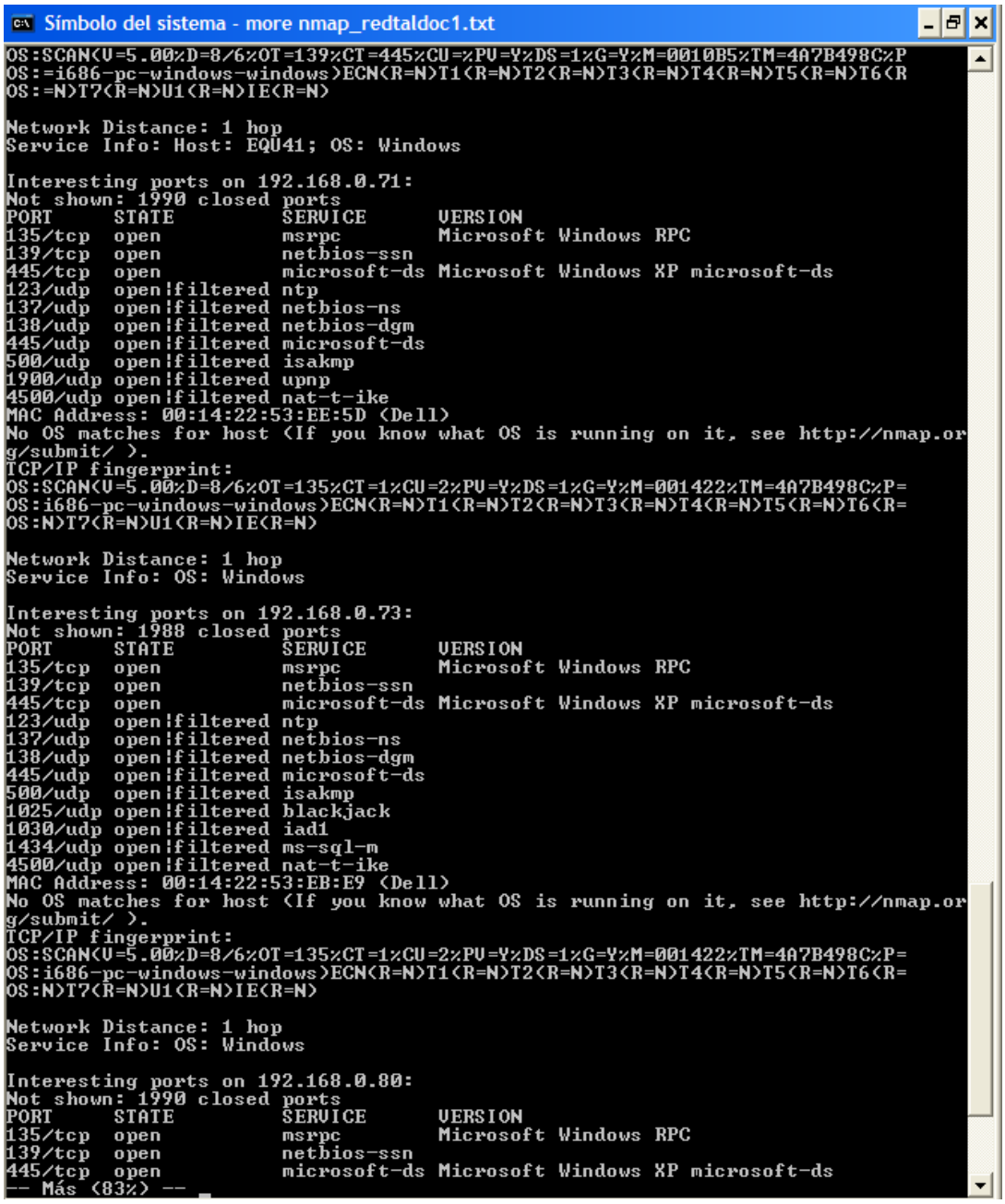


Figura 3.1 nmap

Las herramientas de análisis de vulnerabilidades utilizadas fueron:

- Nessus 4
- Acunetix XSS Scanner
- Nikto Web Server Scanner

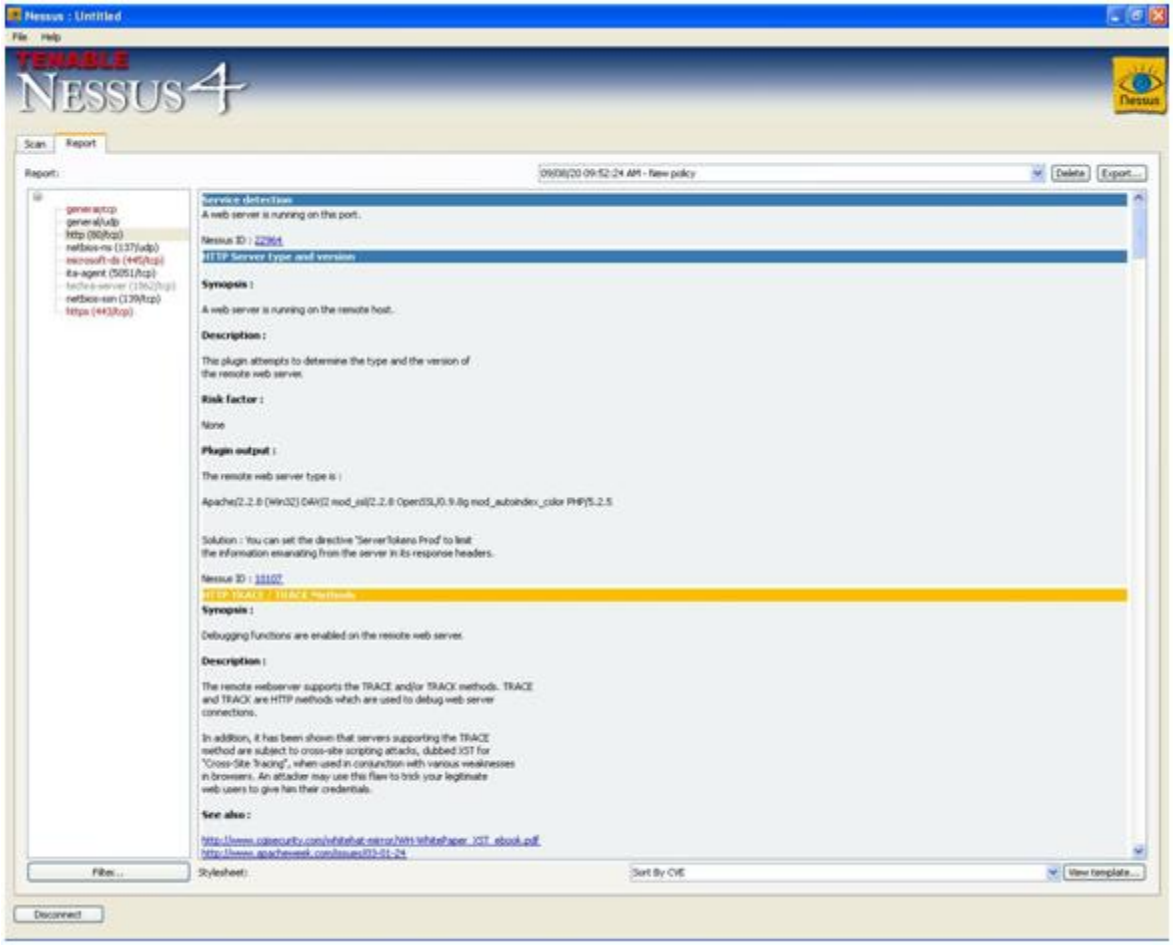


Figura 3.2 Nessus 4

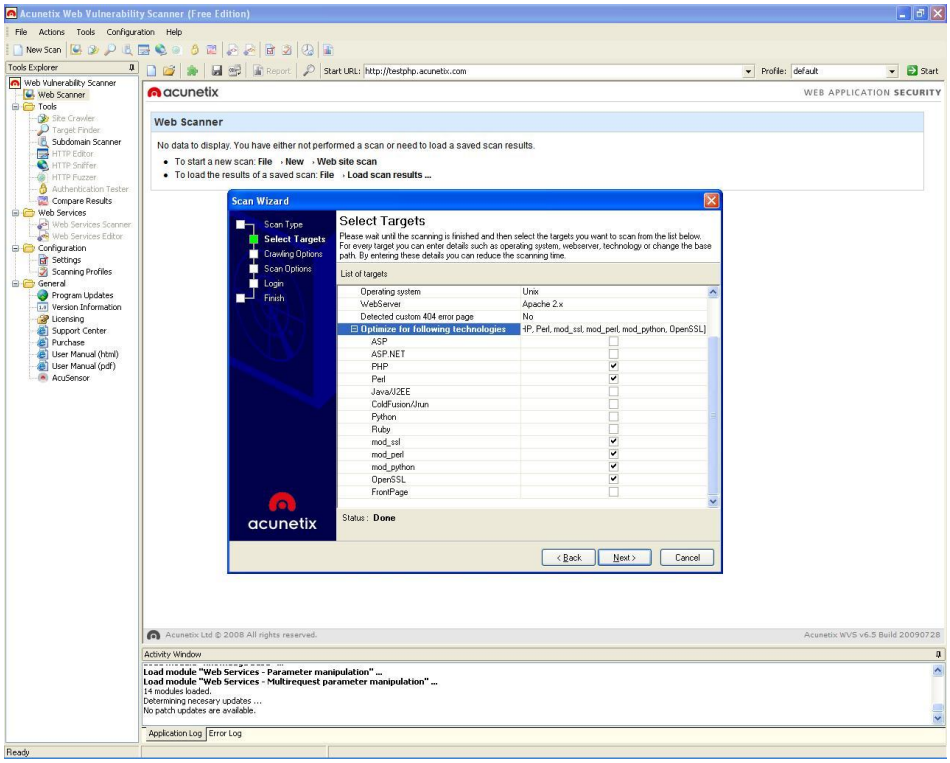


Figura 3.3 Acunetix XSS Scanner

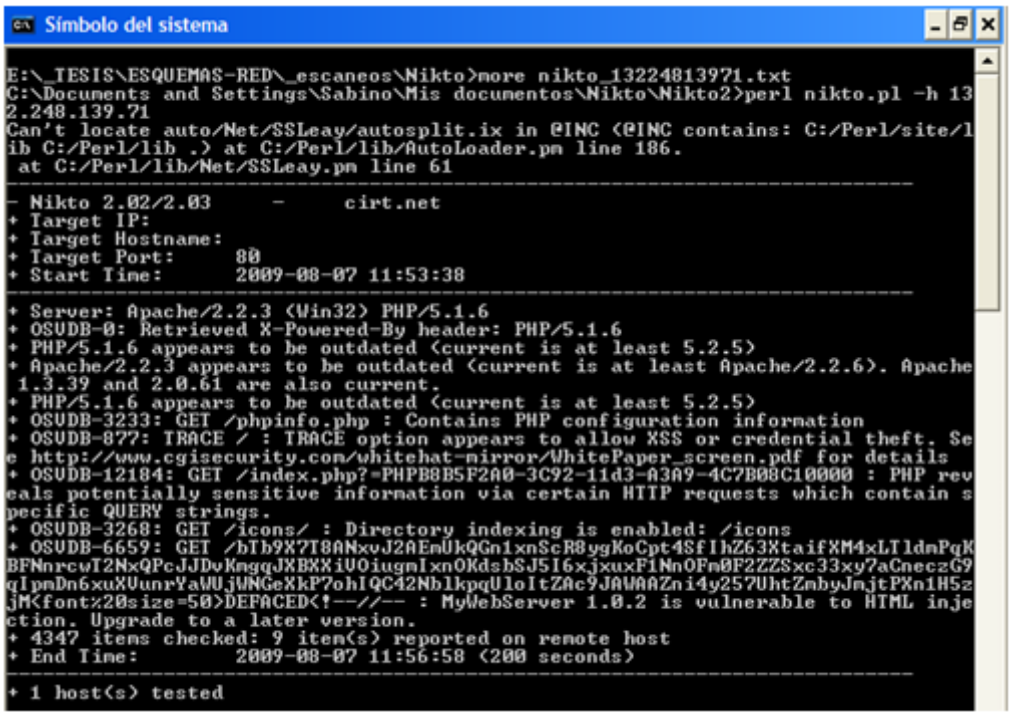
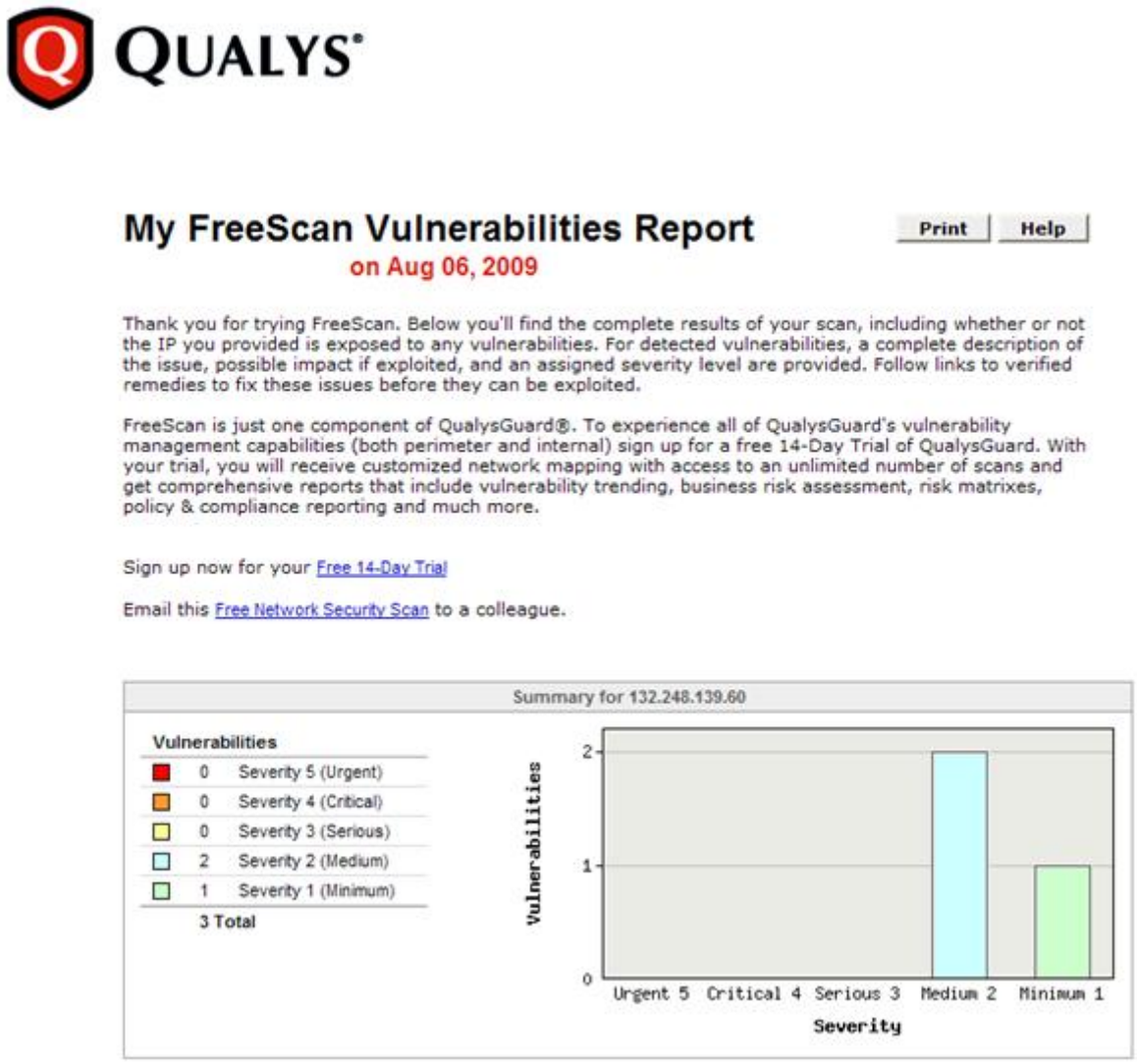


Figura 3.4 Nikto WebServer Scanner

Un reporte elaborado por terceros, a través de la compañía Qualys, utilizando el Qualys FreeScan Vulnerabilities Report.



QUALYS®

My FreeScan Vulnerabilities Report

Print | Help

on Aug 06, 2009

Thank you for trying FreeScan. Below you'll find the complete results of your scan, including whether or not the IP you provided is exposed to any vulnerabilities. For detected vulnerabilities, a complete description of the issue, possible impact if exploited, and an assigned severity level are provided. Follow links to verified remedies to fix these issues before they can be exploited.

FreeScan is just one component of QualysGuard®. To experience all of QualysGuard's vulnerability management capabilities (both perimeter and internal) sign up for a free 14-Day Trial of QualysGuard. With your trial, you will receive customized network mapping with access to an unlimited number of scans and get comprehensive reports that include vulnerability trending, business risk assessment, risk matrixes, policy & compliance reporting and much more.

Sign up now for your Free 14-Day Trial

Email this Free Network Security Scan to a colleague.

Summary for 132.248.139.60

Vulnerabilities	
0	Severity 5 (Urgent)
0	Severity 4 (Critical)
0	Severity 3 (Serious)
2	Severity 2 (Medium)
1	Severity 1 (Minimum)
3 Total	

Figura 3.5 QUALYS FreeScan Vulnerabilities Report

Como resultado se obtuvieron los pares vulnerabilidad/amenaza siguientes:

No.	Vulnerabilidad	Amenaza	Acción
1	Ciertos equipos escuchan en el puerto 137 y contestan a peticiones NetBIOS nbtscan	Usuarios no autorizados	Obtención de nombres de sistema y de dominio
2	Obtención de información de sistema operativo de distintos equipos de la red de la DCB	Usuarios no autorizados	Utilización de distintas herramientas de auditoría
3	Ciertos equipos cuentan con los protocolos CIFS o SMB, utilizados para compartir archivos, carpetas o impresoras dentro de nodos en una red	Usuarios no autorizados	Enumeración de carpetas compartidas dentro de los distintos hosts de la red de la DCB
4	Es posible el acceso a distintos equipos mediante sesiones nulas y/o cuentas de invitado	Usuarios no autorizados	Acceso no autorizado a los equipos
5	Ciertos equipos responden a peticiones SMB para la obtención del host SID	Usuarios no autorizados	Enumeración de usuarios locales
6	Es posible acceder a ciertos equipos mediante usuarios invitados, utilizando cuentas aleatorias	Usuarios no autorizados	Acceso no autorizado a los equipos
7	Ciertos equipos tienen una o más carpetas compartidas de Windows. Dependiendo de los privilegios de dichas carpetas es posible la lectura/escritura remotamente	Usuarios no autorizados	Acceso no autorizado a carpetas compartidas. Modificación a destrucción de información. Alteración de la integridad
8	Ciertos equipos permiten el acceso al Registro de Windows mediante ciertas combinaciones de login / contraseña	Usuarios no autorizados	Acceso no autorizado al registro de Windows

No.	Vulnerabilidad	Amenaza	Acción
9	Mediante ciertas herramientas, es posible identificar archivos compartidos de Office	Usuarios no autorizados	Enumeración de archivos compartidos
10	Posibles conexiones al puerto 1031 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC
11	Posibles conexiones al puerto 2103 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC
12	Posibles conexiones al puerto 1026 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC
13	Posibles conexiones al puerto 2107 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC
14	Posibles conexiones al puerto 2105 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC
15	Posibles conexiones al puerto 135 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC
16	Utilización de herramientas para la identificación del tipo y versión de servidores web	Usuarios no autorizados	Obtención de información de servidores web
17	Los métodos TRACK y TRACE están habilitados en ciertos equipos con servidores web. Son vulnerables a ataques XST (Cross Site Tracking), que pueden ser usados para la obtención sin autorización de credenciales	Usuarios no autorizados	Obtención de credenciales de usuarios mediante XST
18	Es posible la detección de servidores VMWare en ciertos equipos mediante peticiones al puerto 912	Usuarios no autorizados	Mapeo de redes
19	Es posible la detección de servidores web mediante peticiones a los puertos 80 y 443	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
20	Ciertos equipos cuentan con certificados SSL expirados o a expirar prontamente,	Usuarios no autorizados	Falla en autenticación

No.	Vulnerabilidad	Amenaza	Acción
	relacionados a servicios		
21	Ciertos equipos cuentan con protocolos de cifrado de tráfico de red como SSL anticuados (SSLv2)	Usuarios no autorizados	Explotación de vulnerabilidades conocidas en SSL v2
22	Ciertos equipos que utilizan SSL hacen uso de protocolos que realizan cifrados débiles	Usuarios no autorizados	Pérdida de confidencialidad
23	Ciertos equipos son vulnerables a desbordamiento de buffer, que permite ejecutar código arbitrario con los privilegios del sistema	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
24	Ciertos equipos cuentan con vulnerabilidades en SMB de corrupción de memoria, que permiten la ejecución de código arbitrario o una denegación de servicio	Usuarios no autorizados	DoS o ejecución de código arbitrario
25	Ciertos equipos Windows contienen una falla en el servicio de Cliente de Web	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
26	Ciertos equipos Windows contienen una falla en el servicio de cola de impresión	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos

No.	Vulnerabilidad	Amenaza	Acción
27	Ciertos equipos Windows contienen una falla en la implementación SMB	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
28	Ciertos equipos Windows contienen una versión del protocolo SMB (SMBv2), que cuenta con una serie de vulnerabilidades que permiten la ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
29	Ciertos equipos Windows contienen una falla en la intefaz RPC que permite ejecución de código arbitrario y/o lograr privilegios del Sistema	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
30	Ciertos equipos cuentan con servidores web que hacen uso de versiones de PHP obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	Acceso no autorizado, DoS y ejecución de código arbitrario
31	Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	DoS y XSS
32	Ciertos equipos hacen uso de la distribución Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos

No.	Vulnerabilidad	Amenaza	Acción
	desbordamiento de buffer		
33	Es posible la detección de equipos con servicios SMTP activos	Usuarios no autorizados	Envío de spam a través de equipos de la red
34	Ciertos equipos que manejan el protocolo SNMP cuentan con los nombres de comunidades por default (private y public)	Usuarios no autorizados	Cambios no autorizados en configuraciones de equipos
35	Ciertos equipos son vulnerables a ataques de Etherleak (cuando una NIC rellena las tramas con información de paquetes anteriores o con información de la memoria del kernel, en lugar de con bytes nulos)	Usuarios no autorizados	Pérdida de confidencialidad
36	Ciertos equipos reportan las versiones de los servidores web utilizados mediante páginas de error	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
37	Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache Tomcat obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	XSS
38	Es posible la obtención de información de servidores web mediante peticiones al puerto 5353 udp	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
39	Es posible la obtención de información de servidores DNS	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
40	Un servidor DNS responde a	Usuarios no autorizados	DDoS

No.	Vulnerabilidad	Amenaza	Acción
	cualquier petición		
41	Posible identificación de cuentas y servicios mediante el servicio ident (auth)	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
42	Es posible la obtención de información de servidores SSH	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
43	Ciertos equipos que cuentan con el servicio SSH habilitado son vulnerables a ataques de secuestro de sesiones X11	Usuarios no autorizados	Autenticación errónea y/o pérdida de confidencialidad
44	Ciertos servidores cuentan con versiones de SO obsoletas	Usuarios no autorizados	Pérdida de confidencialidad,, integridad, autenticación y disponibilidad
45	En ciertos equipos Windows que cuentan con un servidor de protocolo de escritorio remoto, son vulnerables a ataques de hombre en medio	Usuarios no autorizados	Acceso no autorizado
46	Ciertos equipos Wndows cuentan con el servicio de terminales remotas, que es propenso a ataques de hombre en medio	Usuarios no autorizados	Acceso no autorizado
47	Ciertos equipos con el servicio SSH, cuentan con una versión insegura del protocolo (SSHv1)	Usuarios no autorizados	Pérdida de confidencialidad
48	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que es vulnerable a desbordamientos	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos

No.	Vulnerabilidad	Amenaza	Acción
	de buffer remotos cuando recibe un paquete malicioso SMB		
49	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que permite a un atacante el acceso a archivos arbitrarios fuera de las rutas compartidas permitidas	Usuarios no autorizados	Acceso no autorizado
50	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que, al momento de recibir una petición FindNextPrintChangeNotify() sin haber recibido previamente una llamada FindFirstPrintChangeNoticy() puede ocasionar un DoS	Usuarios no autorizados	DoS
51	Ciertos equipos con el servicio FTP habilitado, permiten que las credenciales de los usuarios sean transmitidas en claro	Usuarios no autorizados	Autenticación errónea y/o pérdida de confidencialidad
52	En ciertos equipos es posible montar volúmenes NFS sin contar con privilegios de root	Usuarios no autorizados	Acceso no autorizado
53	En ciertos equipos con el protocolo FTP habilitado, se permiten accesos anónimos	Usuarios no autorizados	Pérdida de confidencialidad
54	Algunos servidores web son vulnerables a ataques de directorio transversal	Usuarios no autorizados	Pérdida de confidencialidad

No.	Vulnerabilidad	Amenaza	Acción
55	En ciertos equipos es posible listar el software instalado mediante SNMP	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
56	Ciertos equipos tienen instalado Common Management Agent, un componente del manejador de seguridad del sistema de McAfee. Éste contienen una serie de vulnerabilidades que pueden permitir a un atacante causar un DoS, lanzar un ataque de directorio transversal y/o ejecutar código arbitrario	Usuarios no autorizados	DoS, acceso no autorizado y ejecución de código arbitrario desde hosts remotos
57	Ciertos equipos Windows cuentan con versiones del Task Scheduler vulnerables a la ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
58	Ciertos equipos tienen como sistema operativo versiones de MS Windows (Windows 95 / 98 / Me)que ya no son mantenidas por Microsoft, por lo que ya no son publicados parches de seguridad para éstas	Usuarios no autorizados	Explotación de múltiples vulnerabilidades
59	Ciertos equipos tienen habilitada la opción de SMTP relay	Usuarios no autorizados	Envío de spam a través de equipos de la red y posible DoS en la red
60	Es posible la identificación de versiones de los servidores SQL en Windows	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
61	Ciertos equipos responden a peticiones WMI (Windows Management Instrumentation)	Usuarios no autorizados	Mapeo de redes, identificación de objetivos, obtención de credenciales y configuraciónes

No.	Vulnerabilidad	Amenaza	Acción
			de red
62	Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos y DoS
63	Ciertos equipos Windows, cuentan con versiones del servicio Plug and Play que permite la ejecución de código arbitrario y elevación de privilegios	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
64	Es posible la lectura de las bitácoras de eventos en equipos con Windows 2000	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
65	Es posible la enumeración de los servicios que se encuentran activos en equipos Wndows 2000, a través de sesiones nulas	Usuarios no autorizados	Mapeo de redes e identificación de objetivos
66	Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos del Sistema	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
67	Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos

No.	Vulnerabilidad	Amenaza	Acción
68	Existen equipos con servidores web vulnerables a ataques de directorio transversal	Usuarios no autorizados	Acceso no autorizado
69	Ciertos equipos tienen habilitado el servicio de telnet	Usuarios no autorizados	Pérdida de confidencialidad
70	Ciertos equipos tienen instalada una versión de MathCad (12, 13 y 13.1) que es vulnerable a cambios de contraseñas en archivos protegidos, remoción completa de protecciones y acceso a información.	Usuarios no autorizados	Acceso no autorizado a archivos protegidos
71	En la gran mayoría de equipos se tienen instaladas versiones de MS Office que no son actualizadas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Usuarios no autorizados	Pérdida de confidencialidad, integridad, autenticación, y acceso no autorizado.
72	En ciertos equipos se tienen instaladas versiones de Open Office que son obsoletas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Usuarios no autorizados	Pérdida de confidencialidad, integridad, autenticación, y acceso no autorizado.

No.	Vulnerabilidad	Amenaza	Acción
73	En ciertos equipos se tienen instaladas versiones de Autocad (2005 y 2006) que cuenta con una vulnerabilidad no divulgada que permite a un atacante obtener privilegios elevados	Usuarios no autorizados	Acceso no autorizado
74	La mayoría de los equipos tienen instaladas versiones obsoletas de Adobe Acrobat que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	Pérdida de confidencialidad, integridad, autenticación, y acceso no autorizado
75	La gran mayoría de los equipos cuentan con una versión de Kaspersky Antivirus (2008), que cuenta con una vulnerabilidad que permite a un usuario local, obtener privilegios del sistema	Usuarios no autorizados	Elevación de privilegios
76	En ciertos equipos se encuentra instalado Avira Antivir, que cuenta con una vulnerabilidad que permite la elevación de privilegios	Usuarios no autorizados	Elevación de privilegios
77	Ciertos equipos cuentan McAfee Antivirus que cuenta con vulnerabilidades que permiten a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, DoS
78	Ciertos equipos cuentan con Norton Antivirus, que cuenta con vulnerabilidades permiten a la ejecución de código	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, DoS

No.	Vulnerabilidad	Amenaza	Acción
	arbitrario y/o DoS		
79	En ciertos equipos se tienen instaladas versiones de MySQL que cuentan con una serie de vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, DoS, pérdida de integridad, elevación de privilegios, acceso no autorizado
80	En ciertos equipos se tienen instaladas versiones de MSN Live Messenger, que son vulnerables a ataques DoS del servicio	Usuarios no autorizados	DoS
81	En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción de datos	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, pérdida de integridad
82	En ciertos equipos se tienen instalada una versión de Nero Media Player, que es vulnerable a DoS de la aplicación	Usuarios no autorizados	DoS
83	Ciertos equipos cuentan con versiones de Samba (2.2.7) que son vulnerables a ataques de directorio transversal que permiten acceder a directorios protegidos, DoS, ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, acceso no autorizado, DoS
84	Ciertos equipos cuentan con versiones de Samba (3.0.3) que	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, acceso

No.	Vulnerabilidad	Amenaza	Acción
	son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios		no autorizado, DoS
85	Ciertos equipos cuentan con una versión de Apache Tomcat (5.5.26) que es vulnerable a ataques XSS	Usuarios no autorizados	XSS
86	Ciertos equipos cuentan con una versión de Subversion (1.5.1) que es vulnerable a ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos
87	Ciertos equipos cuentan con una versión del proxy Squid (2.5) que es vulnerable a ataques Dos, suplantación de IP, accesos no autorizados y divulgación de información no autorizada	Usuarios no autorizados	DoS, suplantación de IP, acceso no autorizado y pérdida de confidencialidad
88	No se cuenta con una Misión de Seguridad en la DCB	Usuarios autorizados y no autorizados	Violación a la normatividad no formalmente establecida
89	Ciertos funcionarios con altos privilegios a los recursos de la red cuentan con contraseñas débiles	Usuarios autorizados y no autorizados	Se pueden comprometer las credenciales de personal con altos privilegios dentro de la red de la DCB
90	No se cuenta con la debida asignación de responsabilidades en seguridad informática	Usuarios autorizados	Deslinde de responsabilidades

No.	Vulnerabilidad	Amenaza	Acción
91	Ciertos equipos de funcionarios de la DCB no cuentan con controles de acceso para restringir privilegios a ayudantes	Usuarios autorizados	Acceso no autorizado, pérdida de confidencialidad e integridad
92	En el caso de las políticas de seguridad de la Facultad de Ingeniería, no son conocidas por los usuarios de la DCB	Usuarios autorizados	No cumplimiento de las políticas de seguridad que rigen a la FI
93	No se cuentan con políticas escritas de respaldos de información, protección y verificación de éstos	Usuarios autorizados	Pérdida de información en caso de incidentes
94	No se cuentan con políticas escritas de protección a medios de almacenamiento	Usuarios autorizados	Pérdida de confidencialidad e integridad
95	En ciertos servidores y aplicaciones no se lleva un historial de incidentes de seguridad y sus resoluciones	Usuarios autorizados	Posible repetición de un mismo incidente sin que se tomen medidas para evitarlo
96	No se cuentan con políticas escritas de contraseñas	Usuarios autorizados	Pérdida de confidencialidad, integridad y acceso no autorizado
97	No se cuentan con políticas escritas de actualizaciones a sistemas y aplicaciones	Usuarios autorizados	Exposición a vulnerabilidades
98	Cualquier usuario puede instalar aplicaciones en los equipos a los que tienen acceso	Usuarios autorizados	Instalación de software malicioso, no actualizado o con vulnerabilidades

No.	Vulnerabilidad	Amenaza	Acción
			conocidas
99	No se cuenta con control alguno respecto a las aplicaciones que pueden ser instaladas o no en los equipos de la DCB dentro de las áreas de coordinaciones, secciones académicas, laboratorios y cubículos en general	Usuarios autorizados	Instalación de software malicioso, no actualizado o con vulnerabilidades conocidas
100	Existen equipos con información valiosa para la DCB que cuentan con IPs reales, por lo que podrían ser accedidos desde fuera de la red de la División	Usuarios autorizados	Exposición de equipos críticos a redes públicas
101	No se realiza un monitoreo adecuado del tráfico en la red de la DCB	Usuarios autorizados	Posibles intrusiones
102	En ciertos servidores y aplicaciones, el único control de acceso existente es por medio de nombre de usuario y contraseña	Usuarios autorizados	Acceso no autorizado en caso de que las credenciales se vean comprometidas
103	No se cuenta con un correcto inventario de activos informáticos	Usuarios autorizados	Pérdida de activos informáticos
104	No se cuenta con una política de uso aceptable de los recursos informáticos y las sanciones en caso de violar éste a nivel de la DCB	Usuarios autorizados	Mal uso de los recursos informáticos
105	El equipo activo de la DCB cuenta con las contraseñas por default en usuarios privilegiados	Usuarios autorizados	Acceso no autorizado
106	No se cuenta con una clasificación de los recursos informáticos, con base en su nivel crítico y/o sensibilidad	Usuarios autorizados	Pérdida de disponibilidad y/o confidencialidad

No.	Vulnerabilidad	Amenaza	Acción
107	No se cuenta con una capacitación de seguridad adecuada a la mayoría de los usuarios	Usuarios autorizados	Uso indebido de activos, exposición a vulnerabilidades, incumplimiento de políticas
108	No se cuentan con procedimientos de terminación de empleados o cambios de éstos (baja de claves, contraseñas, devolución de activos, privilegios, etc…)	Usuarios autorizados	Acceso no autorizado
109	No se cuenta con equipo específicamente destinado a desarrollo y/o pruebas	Usuarios autorizados	Poner en riesgo los servicios ofrecidos
110	No se cuentan con políticas de gestión de privilegios y revisión periódica de los mismos	Usuarios autorizados	Acceso no autorizado, pérdida de confidencialidad e integridad
111	No se cuentan con políticas documentadas sobre el uso de los servicios de la red	Usuarios autorizados	Uso indebido de los servicios de la red
112	No se cuenta con un control adecuado establecido de conexión de equipos personales a la red	Usuarios autorizados	Acceso no autorizado
113	Los equipos críticos o sensibles de la DCB no se encuentran debidamente segregados	Usuarios autorizados	Acceso no autorizado, DoS, exposición a diversas vulnerabilidades
114	No se cuenta con una política escrita de requerimientos mínimos para el acceso a los servicios de la red	Usuarios autorizados	Exposición a vulnerabilidades
115	La información valiosa para la DCB no es almacenada de	Usuarios autorizados	Pérdida de confidencialidad

No.	Vulnerabilidad	Amenaza	Acción
	forma cifrada		
116	No se cuenta con una debida gestión sobre avisos de vulnerabilidades técnicas que afecten al equipo de la DCB ni los procedimientos de apilcación	Usuarios autorizados	Exposición a vulnerabilidades de publicación reciente
117	No se cuenta con procedimientos escritos en caso de incidentes de seguridad	Usuarios autorizados	Tardanza en la resolución del incidente
118	No se cuenta con una política de realización de estudios de gestión de riesgos	Usuarios autorizados	No hay identificación, mitigación o aceptación de riesgos
119	En caso de falla en el suministro de electricidad prolongado, no hay opción alternativa para continuar con los servicios de la DCB	Falla en el suministro de electricidad	Pérdida de disponibilidad
120	No existe documentación que indique los procedimientos a seguir en caso de aviso previo de falla en el suministro de electricidad	Falla en el suministro de electricidad	Posibles fallas en los servicios de la División
121	No existe documentación que indique los procedimientos a seguir cuando se recupere el suministro de electricidad después de una falla	Falla en el suministro de electricidad	Posibles fallas en los servicios de la División
122	No todos los equipos de la DCB cuentan con sistemas de regulación de voltaje y/o prevención en cortes de energía	Falla en el suministro de electricidad	Posibles fallas en los servicios y/o equipos de la División
123	No existe documentación que indique los procedimientos a seguir antes y después de los periodos de vacaciones administrativas en la División	Usuarios autorizados	Posibles fallas en los servicios de la División

No.	Vulnerabilidad	Amenaza	Acción
124	No existe documentación que indique los procedimientos a seguir antes y después de que ocurra un sismo	Terremotos	Posibles fallas en los servicios de la División
125	No existen procedimientos para el deshecho de documentación valiosa para la DCB	Usuarios no autorizados	Pérdida de confidencialidad
126	No hay control alguno para evitar la suplantación de IPs reales asignadas a la DCB	Usuarios no autorizados	Suplantación
127	Los profesores y alumnos comparten información por medio de dispositivos de almacenamiento como memorias flash, por los cuales se realiza la propagación de virus, spyware, caballos de troya, etc...	Usuarios no autorizados	Exposición a software malicioso

Tabla 3.6 Pares amenaza-vulnerabilidad identificados

3.1.4 Análisis de Controles

- **Controles Técnicos que son utilizados por los sistemas de TI**
  - Listas de IP´s válidas y no permitidas.
  - Controles para el ingreso de usuarios, por ejemplo que sólo un usuario pueda acceder al mismo tiempo y desde un solo navegador.
  - Tiempos de expiración de sesiones.
  - Aplicaciones de protección contra software malicioso.
  - Firewalls implementados mediante netfilter-iptables
  - Acceso a Internet mediante un servidor proxy desde algunos segmentos de red.
  - Uso de máquinas virtuales.
  - Uso de un programa que restituye los equipos cada vez que éstos son reiniciados (Deep Freeze), en salas de cómputo para alumnos y académicos, salones y en algunos equipos de coordinaciones académicas.
  - Programación de formateo y revisión de equipos.
- **Controles de Administración**
  - Permisos de acceso a la red de la DCB sólo a personal académico y administrativo de la División, en caso de que éste requiera hacer uso de equipo propio, tendrá que contar con requisitos mínimos para otorgárseles el acceso.
  - El acceso a los servidores y aplicaciones es discrecional de parte de los administradores.
  - En los equipos de los talleres de cómputo y salones, sólo están permitidos ciertos programas, mientras que en los de coordinaciones, cubículos y áreas administrativas, se tiene un control mínimo de los programas instalados.
  - Programación de mantenimiento preventivo por parte del área administrativa de la Facultad y respuesta a mantenimientos correctivos solicitados.

3.1.5 Determinación de Probabilidad de Ocurrencia

Se asignó un valor de Baja, Media o Alta, para la posible ocurrencia de las vulnerabilidades detectadas, éstas son presentadas en la Tabla 4.2

3.1.6 Análisis de Impacto

Se asignó un valor de Bajo, Medio o Alto, para el impacto que causaría el ejercicio de la vulnerabilidad detectada. Dichos valores son mostrados en la Tabla 4.2

3.1.7 Determinación del Riesgo

Con base en los valores dados de probabilidad de ocurrencia y de análisis de impacto, se realizó la determinación del valor de riesgo para cada par amenaza-vulnerabilidad (identificado por el número asignado en la Tabla 4.1). Se tomó como referencia la matriz de 3 X 3 mostrada en la Figura 3.5

Par Amenaza-Vulnerabilidad	Probabilidad de Ocurrencia	Impacto	Riesgo (Valor)	Nivel de Riesgo
1	Media (0.5)	10	5	Bajo
2	Media (0.5)	10	5	Bajo
3	Media (0.5)	Medio (50)	25	Medio
4	Baja (0.1)	Medio (50)	5	Bajo
5	Baja (0.1)	10	1	Bajo
6	Baja (0.1)	Medio (50)	5	Bajo
7	Alta (1.0)	Medio (50)	50	Medio
8	Media (0.5)	10	5	Bajo
9	Baja (0.1)	10	1	Bajo
10	Baja (0.1)	10	1	Bajo
11	Baja (0.1)	10	1	Bajo
12	Baja (0.1)	10	1	Bajo
13	Baja (0.1)	10	1	Bajo
14	Baja (0.1)	10	1	Bajo
15	Baja (0.1)	10	1	Bajo
16	Media (0.5)	Medio (50)	25	Medio
17	Media (0.5)	Medio (50)	25	Medio
18	Baja (0.1)	10	1	Bajo
19	Alta (1.0)	10	10	Bajo
20	Baja (0.1)	10	1	Bajo
21	Baja (0.1)	10	1	Bajo
22	Baja (0.1)	10	1	Bajo
23	Baja (0.1)	Medio (50)	5	Bajo
24	Baja (0.1)	Medio (50)	5	Bajo
25	Baja (0.1)	10	1	Bajo

Par Amenaza-Vulnerabilidad	Probabilidad de Ocurrencia	Impacto	Riesgo (Valor)	Nivel de Riesgo
26	Baja (0.1)	10	1	Bajo
27	Baja (0.1)	10	1	Bajo
28	Baja (0.1)	10	1	Bajo
29	Baja (0.1)	10	1	Bajo
30	Media (0.5)	Medio (50)	25	Medio
40	Alta (1.0)	Medio (50)	50	Medio
42	Media (0.5)	10	5	Bajo
43	Baja (0.1)	10	1	Bajo
44	Baja (0.1)	10	1	Bajo
45	Baja (0.1)	10	1	Bajo
46	Alta (1.0)	Medio (50)	50	Medio
47	Media (0.5)	10	5	Bajo
48	Baja (0.1)	Medio (50)	5	Bajo
49	Baja (0.1)	10	1	Bajo
50	Baja (0.1)	10	1	Bajo
51	Baja (0.1)	10	1	Bajo
52	Baja (0.1)	10	1	Bajo
53	Baja (0.1)	10	1	Bajo
54	Media (0.5)	10	5	Bajo
55	Baja (0.1)	Medio (50)	5	Bajo
56	Baja (0.1)	10	1	Bajo
57	Baja (0.1)	10	1	Bajo
58	Baja (0.1)	Medio (50)	5	Bajo
59	Media (0.5)	Medio (50)	25	Medio
60	Baja (0.1)	Medio (50)	5	Bajo
61	Baja (0.1)	Medio (50)	5	Bajo
62	Baja (0.1)	10	1	Bajo
63	Media (0.5)	Medio (50)	25	Medio
64	Alta (1.0)	Medio (50)	50	Medio
65	Baja (0.1)	10	1	Bajo
66	Baja (0.1)	10	1	Bajo
67	Baja (0.1)	10	1	Bajo
68	Media (0.5)	10	5	Bajo
69	Baja (0.1)	10	1	Bajo
70	Media (0.5)	10	5	Bajo
71	Baja (0.1)	10	1	Bajo
72	Baja (0.1)	10	1	Bajo
73	Baja (0.1)	10	1	Bajo
74	Baja (0.1)	10	1	Bajo

Par Amenaza-Vulnerabilidad	Probabilidad de Ocurrencia	Impacto	Riesgo (Valor)	Nivel de Riesgo
75	Baja (0.1)	10	1	Bajo
76	Baja (0.1)	10	1	Bajo
77	Baja (0.1)	10	1	Bajo
78	Alta (1.0)	Medio (50)	50	Medio
79	Media (0.5)	Medio (50)	25	Medio
80	Baja (0.1)	10	1	Bajo
81	Alta (1.0)	Medio (50)	50	Medio
82	Media (0.5)	10	5	Bajo
83	Baja (0.1)	10	1	Bajo
84	Media (0.5)	Medio (50)	25	Medio
85	Baja (0.1)	10	1	Bajo
86	Baja (0.1)	10	1	Bajo
87	Baja (0.1)	10	1	Bajo
88	Baja (0.1)	10	1	Bajo
90	Baja (0.1)	10	1	Bajo
91	Media (0.5)	Medio (50)	25	Medio
92	Baja (0.1)	10	1	Bajo
93	Baja (0.1)	10	1	Bajo
94	Baja (0.1)	Medio (50)	5	Bajo
95	Baja (0.1)	Medio (50)	5	Bajo
96	Media (0.5)	10	5	Bajo
97	Baja (0.1)	10	1	Bajo
98	Media (0.5)	Medio (50)	25	Medio
99	Alta (1.0)	**Alto (100)**	100	**Alto**
100	Media (0.5)	Alto (100)	50	Medio
101	Media (0.5)	Medio (50)	25	Medio
102	Alta (1.0)	Medio (50)	50	Medio
103	Alta (1.0)	**Alto (100)**	100	**Alto**
104	Media (0.5)	Medio (50)	25	Medio
105	Media (0.5)	Medio (50)	25	Medio
106	Media (0.5)	10	5	Bajo
107	Alta (1.0)	**Alto (100)**	100	**Alto**
108	Alta (1.0)	**Alto (100)**	100	**Alto**
109	Alta (1.0)	Medio (50)	50	Medio
110	Alta (1.0)	Medio (50)	50	Medio
111	Alta (1.0)	**Alto (100)**	100	**Alto**
112	Media (0.5)	Medio (50)	25	Medio
115	Media (0.5)	Medio (50)	25	Medio
116	Media (0.5)	Medio (50)	25	Medio

Par Amenaza-Vulnerabilidad	Probabilidad de Ocurrencia	Impacto	Riesgo (Valor)	Nivel de Riesgo
117	Alta (1.0)	10	10	Bajo
118	Alta (1.0)	**Alto (100)**	100	**Alto**
119	Baja (0.1)	Medio (50)	5	Bajo
120	Media (0.5)	Medio (50)	25	Medio
121	Alta (1.0)	**Alto (100)**	100	**Alto**
122	Media (0.5)	Medio (50)	25	Medio
123	Media (0.5)	Medio (50)	25	Medio
124	Media (0.5)	10	5	Bajo
125	Alta (1.0)	Medio (50)	50	Medio
127	Media (0.5)	Medio (50)	25	Medio
128	Media (0.5)	Alto (100)	50	Medio
129	Media (0.5)	Medio (50)	25	Medio
130	Media (0.5)	Medio (50)	25	Medio
131	Media (0.5)	10	5	Bajo
132	Media (0.5)	Medio (50)	25	Medio
133	Baja (0.1)	10	1	Bajo
134	Media (0.5)	Alto (100)	50	Medio
135	Media (0.5)	Medio (50)	25	Medio
136	Media (0.5)	Medio (50)	25	Medio
137	Alta (1.0)	Medio (50)	50	Medio
138	Media (0.5)	Medio (50)	25	Medio
139	Baja (0.1)	Medio (50)	5	Bajo
140	Alta (1.0)	Medio (50)	50	Medio
141	Alta (1.0)	Medio (50)	50	Medio
142	Alta (1.0)	Medio (50)	50	Medio

Tabla 3.7 Niveles de Riesgo Obtenido

3.1.8 Recomendación de Controles

Para cada uno de los riesgos obtenidos anteriormente, se realiza una recomendación de uno o varios controles de seguridad basados en el estándar ISO 27002:2005

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
1	Ciertos equipos escuchan en el puerto 137 y contestan a peticiones NetBIOS nbtscan	Usuarios no autorizados	10.6.1 Controles de red
2	Obtención de información de sistema operativo de distintos equipos de la red de la DCB	Usuarios no autorizados	10.6.1 Controles de red
3	Ciertos equipos cuentan con los protocolos CIFS o SMB, utilizados para compartir archivos, carpetas o impresoras dentro de nodos en una red	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
4	Es posible el acceso a distintos equipos mediante sesiones nulas y/o cuentas de invitado	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
5	Ciertos equipos responden a peticiones SMB para la obtención del host SID	Usuarios no autorizados	10.6.1 Controles de red
6	Es posible acceder a ciertos equipos mediante usuarios invitados, utilizando cuentas aleatorias	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
7	Ciertos equipos tienen una o más carpetas compartidas de Windows. Dependiendo de los privilegios de dichas carpetas es posible la lectura/escritura remotamente	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
8	Ciertos equipos permiten el acceso al Registro de Windows mediante ciertas combinaciones de login / contraseña	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
9	Mediante ciertas herramientas, es posible identificar archivos compartidos de Office	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
10	Posibles conexiones al puerto 1031 tcp	Usuarios no autorizados	10.6.1 Controles de red
11	Posibles conexiones al puerto 2103 tcp	Usuarios no autorizados	10.6.1 Controles de red
12	Posibles conexiones al puerto 1026 tcp	Usuarios no autorizados	10.6.1 Controles de red
13	Posibles conexiones al puerto 2107 tcp	Usuarios no autorizados	10.6.1 Controles de red
14	Posibles conexiones al puerto 2105 tcp	Usuarios no autorizados	10.6.1 Controles de red
15	Posibles conexiones al puerto 135 tcp	Usuarios no autorizados	10.6.1 Controles de red
16	Utilización de herramientas para la identificación del tipo y versión de servidores web	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
17	Los métodos TRACK y TRACE están habilitados en ciertos equipos con servidores web. Son vulnerables a ataques XST (Cross Site Tracking), que pueden ser usados para la obtención sin autorización de credenciales	Usuarios no autorizados	5.1.1 Documento de política de seguridad de la información
			11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
18	Es posible la detección de servidores VMWare en ciertos equipos mediante peticiones al puerto 912	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
19	Es posible la detección de	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	servidores web mediante peticiones a los puertos 80 y 443		10.6.1 Controles de red
20	Ciertos equipos cuentan con certificados SSL expirados o a expirar prontamente, relacionados a servicios	Usuarios no autorizados	10.6.1 Controles de red
21	Ciertos equipos cuentan con protocolos de cifrado de tráfico de red como SSL anticuados (SSLv2)	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
22	Ciertos equipos que utilizan SSL hacen uso de protocolos que realizan cifrados débiles	Usuarios no autorizados	10.6.1 Controles de red
23	Ciertos equipos son vulnerables a desbordamiento de buffer, que permite ejecutar código arbitrario con los privilegios del sistema	Usuarios no autorizados	11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
24	Ciertos equipos cuentan con vulnerabilidades en SMB de corrupción de memoria, que permiten la ejecución de código arbitrario o una denegación de servicio	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
25	Ciertos equipos Windows contienen una falla en el servicio de Cliente de Web	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
26	Ciertos equipos Windows contienen una falla en el servicio de cola de impresión	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
27	Ciertos equipos Windows contienen una falla en la implementación SMB	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
28	Ciertos equipos Windows contienen una versión del protocolo SMB (SMBv2), que cuenta con una serie de vulnerabilidades que permiten la ejecución de código arbitrario	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
29	Ciertos equipos Windows contienen una falla en la intefaz RPC que permite ejecución de código arbitrario y/o lograr privilegios del Sistema	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
30	Ciertos equipos cuentan con servidores web que hacen uso de versiones de PHP obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
31	Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
32	Ciertos equipos hacen uso de la distribución Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de desbordamiento de buffer	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
33	Es posible la detección de equipos con servicios SMTP activos	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
34	Ciertos equipos que manejan el protocolo SNMP cuentan con los nombres de comunidades por default (private y public)	Usuarios no autorizados	11.3.1 Uso de contraseñas
			11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
35	Ciertos equipos son vulnerables a ataques de Etherleak (cuando una NIC rellena las tramas con información de paquetes anteriores o con información de la memoria del kernel, en lugar de con bytes nulos)	Usuarios no autorizados	10.6.1 Controles de red
36	Ciertos equipos reportan las versiones de los servidores web utilizados mediante páginas de error	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
37	Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache Tomcat obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
38	Es posible la obtención de información de servidores web mediante peticiones al puerto 5353 udp	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
39	Es posible la obtención de información de servidores DNS	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
40	Un servidor DNS responde a cualquier petición	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
41	Posible identificación de cuentas y servicios mediante el servicio ident (auth)	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
42	Es posible la obtención de información de servidores SSH	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
43	Ciertos equipos que cuentan con el servicio SSH habilitado son vulnerables a ataques de secuestro de sesiones X11	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
44	Ciertos servidores cuentan con versiones de SO obsoletas	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
45	En ciertos equipos Windows que cuentan con un servidor de protocolo de escritorio remoto, son vulnerables a ataques de hombre en medio	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
46	Ciertos equipos Wndows cuentan con el servicio de terminales remotas, que es propenso a ataques de hombre en medio	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
47	Ciertos equipos con el servicio SSH, cuentan con una versión insegura del protocolo (SSHv1)	Usuarios no autorizados	10.6.1 Controles de red
48	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que es vulnerable a desbordamientos de buffer remotos cuando recibe un paquete malicioso SMB	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
49	Ciertos equipos con el servicio Samba habilitado, cuentan con	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	una versión obsoleta que permite a un atacante el acceso a archivos arbitrarios fuera de las rutas compartidas permitidas		11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
50	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que, al momento de recibir una petición FindNextPrintChangeNotify() sin haber recibido previamente una llamada FindFirstPrintChangeNoticy() puede ocasionar un DoS	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
51	Ciertos equipos con el servicio FTP habilitado, permiten que las credenciales de los usuarios sean transmitidas en claro	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
52	En ciertos equipos es posible montar volúmenes NFS sin contar con privilegios de root	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
53	En ciertos equipos con el protocolo FTP habilitado, se permiten accesos anónimos	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
54	Algunos servidores web son vulnerables a ataques de directorio transversal	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
55	En ciertos equipos es posible listar el software instalado mediante SNMP	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
			10.6.1 Controles de red
56	Ciertos equipos tienen instalado Common Management Agent, un componente del manejador de seguridad del sistema de McAfee. Éste contienen una serie de vulnerabilidades que pueden permitir a un atacante causar un DoS, lanzar un ataque de directorio transversal y/o ejecutar código arbitrario	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
57	Ciertos equipos Windows cuentan con versiones del Task Scheduler vulnerables a la ejecución de código arbitrario	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
58	Ciertos equipos tienen como sistema operativo versiones de MS Windows (Windows 95 / 98 / Me)que ya no son mantenidas por Microsoft, por lo que ya no son publicados parches de seguridad para éstas.	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
59	Ciertos equipos tienen habilitada la opción de SMTP relay	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
60	Es posible la identificación de versiones de los servidores SQL en Windows	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
61	Ciertos equipos responden a peticiones WMI (Windows	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	Management Instrumentation)		11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
62	Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
63	Ciertos equipos Windows, cuentan con versiones del servicio Plug and Play que permite la ejecución de código arbitrario y elevación de privilegios	Usuarios no autorizados	11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
64	Es posible la lectura de las bitácoras de eventos en equipos con Windows 2000	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
65	Es posible la enumeración de los servicios que se encuentran activos en equipos Wndows 2000, a través de sesiones nulas	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
66	Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos del Sistema	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
67	Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario		10.3.1 Gestión de la Capacidad
			11.4.2 Autenticación de usuarios para conexiones externa

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
		Usuarios no autorizados	11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
68	Existen equipos con servidores web vulnerables a ataques de directorio transversal	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
69	Ciertos equipos tienen habilitado el servicio de telnet	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			10.6.1 Controles de red
70	Ciertos equipos tienen instalada una versión de MathCad (12, 13 y 13.1) que es vulnerable a cambios de contraseñas en archivos protegidos, remoción completa de protecciones y acceso a información.	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
71	En la gran mayoría de equipos se tienen instaladas versiones de MS Office que no son actualizadas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
72	En ciertos equipos se tienen instaladas versiones de Open Office que son obsoletas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
73	En ciertos equipos se tienen instaladas versiones de Autocad (2005 y 2006) que cuenta con una vulnerabilidad no divulgada que permite a un atacante obtener privilegios elevados	Usuarios no autorizados	10.3.1 Gestión de la Capacidad

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
74	La mayoría de los equipos tienen instaladas versiones obsoletas de Adobe Acrobat que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	10.3.1 Gestión de la Capacidad 10.6.1 Controles de red
75	La gran mayoría de los equipos cuentan con una versión de Kaspersky Antivirus (2008), que cuenta con una vulnerabilidad que permite a un usuario local, obtener privilegios del sistema	Usuarios no autorizados	10.3.1 Gestión de la Capacidad 10.6.1 Controles de red
76	En ciertos equipos se encuentra instalado Avira Antivir, que cuenta con una vulnerabilidad que permite la elevación de privilegios.	Usuarios no autorizados	10.3.1 Gestión de la Capacidad 11.5.4 Uso de los recursos del sistema
77	Ciertos equipos cuentan McAfee Antivirus que cuenta con vulnerabilidades que permiten a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
78	Ciertos equipos cuentan con Norton Antivirus, que cuenta con vulnerabilidades permiten a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
79	En ciertos equipos se tienen instaladas versiones de MySQL que cuentan con una serie de vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado	Usuarios no autorizados	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
80	En ciertos equipos se tienen instaladas versiones de MSN Live Messenger, que son vulnerables a ataques DoS del servicio	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
81	En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción de datos	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
82	En ciertos equipos se tienen instalada una versión de Nero Media Player, que es vulnerable a DoS de la aplicación	Usuarios no autorizados	10.3.1 Gestión de la Capacidad
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
83	Ciertos equipos cuentan con versiones de Samba (2.2.7) que son vulnerables a ataques de directorio transversal que permiten acceder a directorios protegidos, DoS, ejecución de código arbitrario.	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
84	Ciertos equipos cuentan con versiones de Samba (3.0.3) que son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios	Usuarios no autorizados	11.4.1 Política sobre el uso de servicios de red
			11.4.2 Autenticación de usuarios para conexiones externas
			11.5.4 Uso de los recursos del sistema
			10.6.1 Controles de red
85	Ciertos equipos cuentan con una versión de Apache Tomcat (5.5.26) que es vulnerable a ataques XSS	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
86	Ciertos equipos cuentan con una versión de Subversion		11.4.2 Autenticación de usuarios para conexiones

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	(1.5.1) que es vulnerable a ejecución de código arbitrario	Usuarios no autorizados	externas
			10.6.1 Controles de red
87	Ciertos equipos cuentan con una versión del proxy Squid (2.5) que es vulnerable a ataques Dos, suplantación de IP, accesos no autorizados y divulgación de información no autorizada	Usuarios no autorizados	11.4.2 Autenticación de usuarios para conexiones externas
			10.6.1 Controles de red
88	No se cuenta con una Misión de Seguridad en la DCB	Usuarios autorizados y no autorizados	5.1.1 Documento de política de seguridad de la información
89	Ciertos funcionarios con altos privilegios a los recursos de la red cuentan con contraseñas débiles	Usuarios autorizados y no autorizados	5.1.1 Documento de política de seguridad de la información
			11.3.1 Uso de contraseñas
90	No se cuenta con la debida asignación de responsabilidades en seguridad informática	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			6.1.3 Asignación de responsabilidades relativas a las seguridad de la información
91	Ciertos equipos de funcionarios de la DCB no cuentan con controles de acceso para restringir privilegios a ayudantes	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			11.5.1 Procedimientos seguros de inicio de sesión
			11.5.2 Identificación y autenticación de usuario
92	En el caso de las políticas de seguridad de la Facultad de Ingeniería, no son conocidas por los usuarios de la DCB	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
93	No se cuentan con políticas escritas de respaldos de información, protección y	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.5.1 Copias de seguridad de la información

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	verificación de éstos		10.7.1 Gestión de medios removibles
			10.7.3 Procedimientos de manipulación de la información
94	No se cuentan con políticas escritas de protección a medios de almacenamiento	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.7.1 Gestión de medios removibles
			10.7.3 Procedimientos de manipulación de la información
			11.1.1 Políticas de control de acceso
95	En ciertos servidores y aplicaciones no se lleva un historial de incidentes de seguridad y sus resoluciones	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.10.1 Registro de auditoría
			13.2.2 Aprendizaje de los incidentes de seguridad de la información
96	No se cuentan con políticas escritas de contraseñas	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			11.3.1 Uso de contraseñas
97	No se cuentan con políticas escritas de actualizaciones a sistemas y aplicaciones	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
98	Cualquier usuario puede instalar aplicaciones en los equipos a los que tienen acceso	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.10.2 Supervisión del uso de sistema
99	No se cuenta con control alguno respecto a las aplicaciones que pueden ser instaladas o no en los equipos	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.10.2 Supervisión del uso de sistema

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	de la DCB dentro de las áreas de coordinaciones, secciones académicas, laboratorios y cubículos en general.		10.4.1 Controles contra el código malicioso
100	Existen equipos con información valiosa para la DCB que cuentan con IPs reales, por lo que podrían ser accedidos desde fuera de la red de la División	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.6.1 Controles de red
101	No se realiza un monitoreo adecuado del tráfico en la red de la DCB	Usuarios autorizados	10.6.1 Controles de red
102	En ciertos servidores y aplicaciones, el único control de acceso existente es por medio de nombre de usuario y contraseña	Usuarios autorizados	11.3.1 Uso de contraseñas
103	No se cuenta con un correcto inventario de activos informáticos	Usuarios autorizados	7.1.1 Inventario de activos
			7.1.2 Propiedad de los activos
104	No se cuenta con una política de uso aceptable de los recursos informáticos y las sanciones en caso de violar éste a nivel de la DCB	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			7.1.3 Uso aceptable de los activos
105	El equipo activo de la DCB cuenta con las contraseñas por default en usuarios privilegiados	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			11.3.1 Uso de contraseñas
106	No se cuenta con una clasificación de los recursos informáticos, con base en su nivel crítico y/o sensibilidad	Usuarios autorizados	7.2.1 Directrices de clasificación
			7.2.2 Etiquetado y manipulación de la información
107	No se cuenta con una capacitación de seguridad	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
	adecuada a la mayoría de los usuarios		8.2.2 Concienciación, formación y capacitación en seguridad de la información
108	No se cuentan con procedimientos de terminación de empleados o cambios de éstos (baja de claves, contraseñas, devolución de activos, privilegios, etc…)	Usuarios autorizados	8.3.1 Responsabilidad del cese o cambio
			8.3.2 Devolución de activos
			8.3.3 Retiro de los derechos de acceso
109	No se cuenta con equipo específicamente destinado a desarrollo y/o pruebas	Usuarios autorizados	10.1.4 Segregación de los recursos de desarrollo, prueba y operación
110	No se cuentan con políticas de gestión de privilegios y revisión periódica de los mismos	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			11.1.1 Políticas de control de acceso
111	No se cuentan con políticas documentadas sobre el uso de los servicios de la red	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			7.1.3 Uso aceptable de los activos
			11.4.1 Política sobre el uso de servicios de red
112	No se cuenta con un control adecuado establecido de conexión de equipos personales a la red	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			11.4.6 Control de la conexión a la red
113	Los equipos críticos o sensibles de la DCB no se encuentran debidamente segregados	Usuarios autorizados	11.4.5 Segregación de las redes
114	No se cuenta con una política escrita de requerimientos mínimos para el acceso a los servicios de la red	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			10.3.1 Gestión de la Capacidad
			10.3.2 Aceptación del sistema
115	La información valiosa para la DCB no es almacenada de forma cifrada	Usuarios autorizados	10.8.1 Políticas y procedimientos de intercambio de información

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
116	No se cuenta con una debida gestión sobre avisos de vulnerabilidades técnicas que afecten al equipo de la DCB ni los procedimientos de aplicación	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
117	No se cuenta con procedimientos escritos en caso de incidentes de seguridad	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
			13.1.1 Notificación de los eventos de seguridad de la información
118	No se cuenta con una política de realización de estudios de gestión de riesgos	Usuarios autorizados	5.1.1 Doc. de políticas. de seg. de la información
			14.1.2 Continuidad del negocio y evaluación de riesgos
119	En caso de falla en el suministro de electricidad prolongado, no hay opción alternativa para continuar con los servicios de la DCB	Falla en el suministro de electricidad	9.2.2 Instalaciones de suministro
120	No existe documentación que indique los procedimientos a seguir en caso de aviso previo de falla en el suministro de electricidad	Falla en el suministro de electricidad	9.2.2 Instalaciones de suministro
121	No existe documentación que indique los procedimientos a seguir cuando se recupere el suministro de electricidad después de una falla	Falla en el suministro de electricidad	9.2.2 Instalaciones de suministro
122	No todos los equipos de la DCB cuentan con sistemas de regulación de voltaje y/o prevención en cortes de energía	Falla en el suministro de electricidad	9.2.2 Instalaciones de suministro

No.	Vulnerabilidad	Amenaza	Recomendación de Controles (ISO 27002:2005)
123	No existe documentación que indique los procedimientos a seguir antes y después de los periodos de vacaciones administrativas en la División	Usuarios autorizados	5.1.1 Documento de política de seguridad de la información
124	No existe documentación que indique los procedimientos a seguir antes y después de que ocurra un sismo	Terremotos	9.1.4 Protecciones contra las amenazas externas y de origen ambiental
125	No existen procedimientos para el deshecho de documentación valiosa para la DCB	Usuarios no autorizados	5.1.1 Documento de política de seguridad de la información
126	No hay control alguno para evitar la suplantación de IPs reales asignadas a la DCB	Usuarios no autorizados	10.6.1 Controles de red
127	Los profesores y alumnos comparten información por medio de dispositivos de almacenamiento como memorias flash, por los cuales se realiza la propagación de virus, spyware, caballos de troya, etc...	Usuarios no autorizados	10.4.1 Controles contra el código malicioso

Tabla 3.8 Recomendación de Controles de acuerdo con el ISO 27002:200

Descripción de los controles:

- **5.1.1 Documento de la política de seguridad de la información**

  El documento de las políticas de seguridad de la información deberá ser aprobado por el Jefe de la División, publicado y comunicado a todos los empleados y a las partes externas relevantes.

  Deberá de enunciar el compromiso de la jefatura y establecer el enfoque de la DCB para manejar la seguridad de la información.

- **6.1.3 Asignación de responsabilidades relativas a las seguridad de la información**

Todas las responsabilidades de la seguridad de la información deberán estar claramente definidas.

- **7.1.1 Inventario de activos**

Se deberán de identificar todos los activos, además de elaborar y mantener un inventario de todos los activos importantes.

- **7.1.2 Propiedad de los activos**

Toda la información y los activos asociados con los medios de procesamiento de información deberán ser propiedad de alguna parte designada por la DCB.

- **7.1.3 Uso aceptable de los activos**

Se deberán identificar e implantar reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento ésta en concordancia con la misión de la DCB.

- **7.2.1 Directrices de clasificación**

Se deberá clasificar la información en términos de su valor, requerimientos legales, sensibilidad y nivel crítico para la División.

- **7.2.2 Etiquetado y manipulación de la información**

Se deberá desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización

- **8.2.2 Concientización, formación y capacitación en seguridad de la información**

  Todo el personal de la DCB, y cuando sea relevante, los contratistas y terceras personas deberán recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

- **8.3.1 Responsabilidad del cese o cambio**

  Se deberán definir y asignar claramente las responsabilidades de realizar la terminación o cambio de la plaza.

- **8.3.2 Devolución de activos**

  Todo el personal de la DCB deberá devolver todos los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo.

- **8.3.3 Retiro de los derechos de acceso**

  Los derechos de acceso de todos el personal de la DCB y terceras personas a la información y los medios de procesamiento de información deberán ser retirados a la terminación de su empleo, contrato o acuerdo, o deberán ser reajustados de acuerdo al cambio.

- **9.1.4 Protecciones contra las amenazas externas y de origen ambiental**

  Se deberán asignar y aplicar protecciones contra daño por fuego, inundación, terremoto, explosión, huelga y otras formas de desastres naturales o causados por el hombre.

- **9.2.2 Instalaciones de suministro**

  Se deberá proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

- **10.3.1 Gestión de la Capacidad**

  Se deberá monitorear y afinar el uso de recursos, y se deberán realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

- **10.3.2 Aceptación del sistema**

  Se deberá establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas, y se deberán realizar pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación en la DCB.

- **10.4.1 Controles contra el código malicioso**

  Deberán establecerse controles de detección y prevención de código malicioso, así como controles de recuperación y protección en caso de daño. Así como los procedimientos correspondientes en la DCB.

- **10.5.1 Copias de seguridad de la información**

  Se deberán realizar copias de seguridad de la información y software, además de probarse regularmente. El medio de almacenamiento tendrá que ser protegido de la misma manera que la información original, además de que deberá de revisarse éste periódicamente, para que así, en caso de necesitarse, se tenga la certeza de que es correcto el respaldo requerido.

- **10.6.1 Controles de red**

  Las redes deberán ser adecuadamente manejadas y controlada para poder proteger la información en las mismas y mantener la seguridad de los sistemas y aplicaciones utilizadas dentro de la DCB, incluyendo la información en tránsito.

  Deberán de revisarse y actualizarse los firewalls colocados en el área del Taller para la Docencia y en el Taller de Cómputo para Académicos.

Además de colocar un IDS a la entrada de la red de la DCB, o en su defecto, a la altura del switch 5500 ubicado en el Taller de Cómputo para Académicos, se sugiere el programa Snort, ya que es el estándar de facto en los sistemas de detección de intrusos, además de ser libre.

Así mismo de establecer un programa de monitoreo en tiempo real, en el mismo sitio que el IDS. Se sugiere el programa ntop, ya que con éste se pueden obtener estadísticas de uso (pudiendo ser mostrados por minutos, horas, días o semanas), tipo de tráfico, sitios web visitados, entre otras.

- **10.7.1 Gestión de medios removibles**

En el caso de baja o cambio de equipo que maneje información valiosa para la DCB, el disco duro deberá de ser formateado mínimo diez veces, para que así no pueda ser recuperada la información y sea divulgada a usuarios no autorizados.

Además se requiere la elaboración de procedimientos de gestión de los medios removibles y su información contenida, como discos duros, CD´s, DVD´s, etc.

- **10.7.3 Procedimientos de manipulación de la información**

Se deberán establecer procedimientos para el manejo y almacenamiento de información en la DCB, para proteger dicha información de una divulgación no autorizada o mal uso.

- **10.8.1 Políticas y procedimientos de intercambio de información**

Se deberán establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través de los distintos medios de comunicación.

- **10.1.4 Segregación de los recursos de desarrollo, prueba y operación**

Los equipos de desarrollo, prueba y operación deberán estar separados para reducir los riesgos de acceso no autorizado o cambios en el sistema operacional.

Por lo que se deberán de asignar los recursos necesarios para dichas tareas, así como establecer los responsables y privilegios de éstos.

- **10.10.1 Registro de auditoría**

Se deberán producir y mantener registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso a la información.

- **10.10.2 Supervisión del uso de sistema**

Se deberán establecer procedimientos para el monitoreo del uso de los medios de procesamiento de la información y se deberán revisar regularmente los resultados de las actividades de monitoreo mediante la implantación de candados en los sistemas operativos y/o aplicaciones.

- **11.1.1 Políticas de control de acceso**

Se deberán establecer, documentar y revisar las políticas de control de acceso en base a los requerimientos de la División.

- **11.3.1 Uso de contraseñas**

Se deberá requerir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de contraseñas.

Algunas buenas prácticas son: mantenerlas confidenciales, no tenerlas en algún documento (en papel o digital), cambiarlas cuando se tenga la menor sospecha de que han sido divulgadas, cambiarlas regularmente, que tengan una longitud igual o mayor a 10 caracteres, que no estén basadas en información personal o en palabras de diccionario, no usar la misma contraseña para distintos propósitos y que no sean secuencias ya sea de números o letras, o de letras en el teclado.

- **11.4.1 Política sobre el uso de servicios de red**

  El personal de la DCB sólo deberá tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

- **11.4.2 Autenticación de usuarios para conexiones externas**

  Se deberán utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos. Para esto, deberán de implantarse controles de red tales como VPN´s o canales seguros cuando sean requeridos.

- **11.4.5 Segregación de las redes**

  Los grupos de servicios de información, usuarios y sistemas de información deberán ser segregados en subredes. Además de que deberá de asegurarse que dichas subredes no puedan tener acceso a los recursos de otras, sin el consentimiento previo.

- **11.4.6 Control de la conexión a la red**

  Se deberá de documentar un procedimiento para la conexión de equipo propio del personal académico-administrativo, y los requerimientos mínimos para su aceptación, además de establecer criterios para que éstos puedan contar con el acceso.

- **11.5.1 Procedimientos seguros de inicio de sesión**

  El acceso a los sistemas operativos deberá ser controlado mediante un procedimiento de registro seguro. Se deberá de contar mínimo con una autenticación de usuario / contraseña en el caso de equipo con información valiosa para la DCB.

- **11.5.2 Identificación y autenticación de usuario**

  Todos los usuarios tienen un identificador único para su uso personal, y se deberá escoger una técnica de autenticación adecuada para determinar la identidad de un usuario.

- **11.5.4 Uso de los recursos del sistema**

  Se deberá restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación. Es decir, para aplicaciones que manejen información o datos sensibles, ya sea para los equipos donde se está trabajando o para la DCB, se deberá de tener un control de acceso adecuado.

- **13.1.1 Notificación de los eventos de seguridad de la información**

  Se deberá de elaborar un procedimiento para la oportuna notificación, registro y solución de incidentes de seguridad en la DCB.

- **13.2.2 Aprendizaje de los incidentes de seguridad de la información**

  Se deberán establecer mecanismos para permitir cuantificar y monitorear los incidentes en la seguridad de la información en la DCB.

- **14.1.2 Continuidad del negocio y evaluación de riesgos**

  Se deberá establecer una política de elaboración de estudios de gestión de riesgos periodica.

3.1.9 Documentación de Resultados

La documentación correspondiente al proceso de evaluación de riesgos es presentada en el Anexo III *Documentación de las Actividades de Análisis de Riesgo.*

3.2 Mitigación de Riesgos

En este punto se realizan los puntos descritos en la Figura 3.5, que comprenden el segundo proceso de la gestión de riegos.

3.2.1 Priorización de Acciones

Tomando como referencia el proceso de evaluación de riesgos, se puede observar cuáles son los riesgos que hay que abordar con urgencia, y cuáles pueden serlo a mediano plazo.

Se tomaron como parámetros para otorgar un valor de prioridad de los controles a implantar, el valor de los riesgos relacionados con los controles propuestos, así como el número de riesgos en los que dicho control está relacionado.

Se utilizó una escala de valores de acuerdo a su prioridad de Alta, Media y Baja, de acuerdo con los siguientes criterios:

- **Prioridad Alta**. Se considera con sólo riesgo cuyo nivel sea alto.
- **Prioridad Media**. Con riesgos de nivel Medio y/o Bajo y un número de riesgos asociado mayor o igual a dos.
- **Prioridad Baja**. Con riesgos de nivel Medio y/o Bajo y un número de riesgos asociado igual a uno. O bien, riesgos de nivel Bajo y un número de ocurrencia mayor a uno.

- **Alta**

5.1.1 Documento de la política de seguridad

7.1.3 Uso aceptable de los activos

8.2.2 Concientización, formación y capacitación en seguridad de la información

11.1.1 Política de control de acceso

11.3.1 Uso de contraseñas

11.4.1 Política sobre uso de los servicios de red

- **Media**

9.2.2 Instalación de suministro

10.3.1 Gestión de capacidades

10.6.1 Controles de red

10.7.1 Gestión de medios removibles

10.7.3 Procedimientos de manipulación de la información

10.10.2 Supervisión del uso del sistema

10.4.1 Controles contra el código malicioso

11.4.2 Autenticación de usuarios para conexiones externas

11.5.4 Uso de los recursos del sistema

- **Baja**

6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

7.1.1 Inventario de activos

7.1.2 Propiedad de activos

7.2.1 Directrices de clasificación

7.2.2 Etiquetado y manipulación de la información

8.3.1 Responsabilidad del cese o cambio

8.3.2 Devolución de activos

8.3.3 Retiro de los derechos de acceso

9.1.4 Protección contra amenazas externas y de origen ambiental

10.1.4 Separación de los recursos de desarrollo, prueba y operación

10.5.1 Copias de seguridad de la información

10.8.1 Políticas y procedimientos de intercambio de información

10.10.1 Registro de auditorías

10.3.2 Aceptación del sistema

11.4.5 Segregación de las redes

11.4.6 Control de la conexión a la red

11.5.1 Procedimientos seguros de inicio de sesión

11.5.2 Identificación y autenticación de usuario

13.1.1 Notificación de los eventos de seguridad de la información

13.2.2 Aprendizaje de los incidentes de seguridad de la información

14.1.2 Continuidad del negocio y evaluación de riesgos

3.2.2 Evaluación de las opciones de controles recomendados

Debido a la naturaleza de los controles propuestos en el estándar ISO 27002:2005 (de ser controles generales, aplicables a cualquier tipo de organización, incluyendo una de enseñanza como lo es la DCB), todos los controles propuestos son fiables y efectivos para su aplicación en la División, por lo que se realizará al análisis costo-beneficio para cada uno de ellos.

3.2.3 Análisis costo-beneficio

Se analizaron los controles propuestos mediante un enfoque cualitativo, se tomaron en cuenta parámetros como el posible impacto de la implantación y la no implantación de éstos, así como el costo potencial de su implantación para el cual se consideró lo siguiente: el personal asignado y el posible personal extra requerido, la capacitación, el software relacionado (en los controles que aplique), su mantenimiento, su mantenimiento y la adquisición de hardware.

Además de buscar cumplir el principio de proporcionalidad, que indica que el costo de implantar controles que busquen proteger cierta información no debe ser mayor al costo de la información misma, o al costo en caso de pérdida o divulgación.

Para la determinación del costo estimado, se tomó como referencia lo siguiente:

1. El personal asignado:

   Alto: Dos o más personas de tiempo completo por periodos superiores a dos semanas.

   Medio: Una persona de tiempo completo por periodos superiores a dos semanas.

   Bajo: Una persona por un periodo menor a dos semanas.

2. Personal extra requerido:

   Alto: Se requiere por periodos superiores a dos semanas.

   Medio: Se requiere por un periodo máximo de dos semanas.

   Bajo: No se requiere.

3. Capacitación.

   Alto: Genera un gasto extra e implica la contratación de terceros.

   Medio: Genera un gasto extra.

   Bajo: Se realiza por parte del personal de la División.

4. Software relacionado:

   Alto: Adquisición de software especializado de alto costo.

   Medio: Adquisición de software especializado.

   Bajo: Utilización de software libre o no se requiere.

5. Mantenimiento:

   Alto: Se requiere la contratación de terceros para llevarlo a cabo y además genera un costo.

   Medio: Se realiza por parte del personal de la DCB en más de dos ocasiones por semana.

   Bajo: Se realiza por parte del personal de la DCB una vez a la semana.

6. Adquisición de hardware:

   Alto: Se requiere la adquisición de equipo especializado de alto costo.

   Medio: Se requiere la adquisición de equipo de cómputo.

   Bajo: No se requiere la adquisición.

Considerando los puntos previamente mencionados, para la determinación del costo estimado se utilizaron los siguientes parámetros:

Costo estimado Alto: Dos o más puntos con nivel Alto.

Costo estimado Medio: Máximo un punto con nivel Alto y dos o más con nivel Medio.

Costo estimado Bajo: Máximo un punto con nivel Alto y máximo uno con nivel Medio.

PRIORIDAD DE ACCIÓN ALTA	**Impacto de la Implantación**	**Impacto de la NO Implantación**	**Estimación del costo de implantación**
5.1.1 Documento de la política de seguridad	Alto	Alto	Bajo
7.1.3 Uso aceptable de los activos	Alto	Alto	Bajo
8.2.2 Concientización, formación y capacitación en seguridad de la información	Alto	Medio	Bajo
11.1.1 Política de control de acceso	Alto	Medio	Bajo
11.3.1 Uso de contraseñas	Alto	Medio	Bajo
11.4.1 Política sobre uso de los servicios de red	Alto	Medio	Bajo

Tabla 3.91 Pares amenaza-vulnerabilidad identificados

PRIORIDAD DE ACCIÓN MEDIA	**Impacto de la Implantación**	**Impacto de la NO Implantación**	**Estimación del costo de implantación**
9.2.2 Instalación de suministro	Baja	Media	Bajo
10.3.1 Gestión de capacidades	Baja	Baja	Bajo
10.6.1 Controles de red (IDS, IPS, firewall)	Alta	Baja	Medio
10.7.1 Gestión de medios removibles	Baja	Baja	Medio
10.7.3 Procedimientos de manipulación de la información	Media	Baja	Bajo
10.10.2 Supervisión del uso del sistema	Baja	Baja	Bajo
10.4.1 Controles contra el código malicioso	Media	Media	Bajo
11.4.2 Autenticación de usuarios para conexiones externas	Baja	Media	**Alto**
11.5.4 Uso de los recursos del sistema	Media	Baja	Bajo

Tabla 3.10 Pares amenaza-vulnerabilidad identificados

PRIORIDAD DE ACCIÓN BAJA	**Impacto de la Implantación**	**Impacto de la NO Implantación**	**Estimación del costo de implantación**
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	Baja	Baja	Bajo
7.1.1 Inventario de activos	Baja	Media	Bajo
7.1.2 Propiedad de activos	Baja	Media	Bajo
7.2.1 Directrices de clasificación	Media	Baja	Bajo
7.2.2 Etiquetado y manipulación de la información	Media	Baja	Bajo
8.3.1 Responsabilidad del cese o cambio	Baja	Baja	Bajo
8.3.2 Devolución de activos	Baja	Baja	Bajo
8.3.3 Retiro de los derechos de acceso	Baja	Media	Bajo
9.1.4 Protección contra amenazas externas y de origen ambiental	Baja	Media	Bajo
10.1.4 Separación de los recursos de desarrollo, prueba y operación	Media	Baja	Medio
10.8.1 Políticas y procedimientos de intercambio de información	Alto	Medio	Bajo
10.10.1 Registro de auditorías	Media	Media	Bajo
10.3.2 Aceptación del sistema	Baja	Baja	Bajo
10.5.1 Copias de seguridad de la información	Alto	Medio	Medio
11.4.5 Segregación de las redes	Media	Baja	Medio
11.4.6 Control de la conexión a la red	Baja	Baja	Bajo
11.5.1 Procedimientos seguros de inicio de sesión	Media	Baja	Medio
11.5.2 Identificación y autenticación de usuario	Baja	Baja	Bajo
13.1.1 Notificación de los eventos de seguridad de la información			Bajo
13.2.2 Aprendizaje de los incidentes de seguridad de la información	Baja	Media	Bajo
14.1.2 Continuidad del negocio y evaluación de riesgos	Baja	Baja	Bajo

Tabla 3.11 Pares amenaza-vulnerabilidad identificados

3.2.4 Selección de Controles

Debido a que ningún control tiene un costo de implantación alto, y son aplicables, fiables y efectivos, en el contexto de la DCB, se hará la propuesta de 35 controles, únicamente dejando fuera el control 11.4.2 (Autenticación de usuarios para conexiones externas, ya que su costo de implantación es elevado y en caso de ser llevado a cabo de manera incorrecta, tendría un severo impacto negativo en la red de la División.

3.2.5 Asignación de Responsabilidades

Se designaron distintas entidades para que sean responsables de los controles seleccionados, éstas son:

- Jefe de la División (JD).
- Consejo Interno de Planeación Permanente de la DCB (CIPP).
- Coordinador de Cómputo (CC).
- Administrador de Red (AR).
- Responsables del Taller de Cómputo para Académicos (RTCA).

3.2.6 Programa de Implantación de la Propuesta

En el Anexo IV *Documentación de las Actividades de la Mitigación de Riesgos*, se muestra el programa de implantación propuesto de los distintos controles seleccionados, donde se indica su prioridad, los riesgos y su nivel asociado, el personal responsable de dicha implantación, el tiempo estimado y comentarios.

3.2.7 Implantación de los Controles Seleccionados y Riesgos Residuales

La implantación de la propuesta en la DCB, está condicionada a la aprobación de los responsables de la División de Ciencias Básicas, razón por la cual en el programa propuesto no se especifican fechas de inicio y término de la implantación de los distintos controles, además de que el tiempo estimado sugerido es subjetivo dado del desconocimiento de los recursos con los que se contaría para su implantación.

Los riesgos residuales serán aquellos que, el terminar el programa de implantación, se hayan reducido a Bajo, y que además el impacto potencial pueda ser asumido sin afectar la misión y actividades de la DCB.

3.3 CUESTIONARIO PARA LA CARACTERIZACIÓN DE LOS SERVIDORES Y EQUIPO ACTIVO DE LA RED DE CÓMPUTO DE LA DCB DE LA UNAM

1. Sistema operativo y versión que utiliza _____
2. Versión del kernel (en caso de que aplique) _____
3. IP y su alias _____
4. Servicios que proporciona el servidor (ejemplo: web, Apache 2.2.10)

Servicio	Programa	Versión

5. ¿El servidor cuenta con alguna medida de seguridad física para su acceso? En caso afirmativo, indique
6. Requerimientos de disponibilidad del servidor

(disponibilidad: propiedad de ser accesible y utilizable a petición por entidades autorizadas)

- □ Siempre disponible
- □ Días y horas hábiles
- □ Otro : _____

7. Requerimientos de disponibilidad de la información
   - □ Siempre disponible
   - □ Días y horas hábiles
   - □ Otro : _____
8. Requerimientos de integridad de la información (integridad: propiedad de la información que asegura que ésta no ha sido alterada o destruida de manera no autorizada)

Seleccione una:

- Importancia Crítica
- Importancia Alta
- Importancia Media
- Importancia Baja

9. Requerimientos de confidencialidad de la información (confidencialidad: propiedad de la información que asegura que ésta no se encuentra disponible o es divulgada hacia individuos, entidades o procesos no autorizados)

Seleccione una o varias:

- Información Confidencial
- Información Interna
- Información Pública

10. Tipo de información que maneja
11. Información que se genera (de salida), requiere (de entrada), se procesa y es almacenada por el servidor
12. Importancia de la información que maneja el servidor para la DCB. Expliqué el por qué de su respuesta
    - Importancia Crítica
    - Importancia Alta
    - Importancia Media
    - Importancia Baja
13. ¿Qué información manejada por el servidor o a punto de ser manejada por éste, no debe ser divulgada y a quiénes?
14. ¿Cuál es el impacto potencial si la información es divulgada a personal no autorizado?
15. ¿Cuál es el efecto que causaría en la DCB si el servidor no es fiable?
16. ¿Qué valor le asignaría a la información que maneja el servidor?

Seleccione una:

- Valor Crítico
- Valor Alto
- Valor Medio
- Valor Bajo

17. ¿Cuánto tiempo de inactividad del servidor se puede tolerar en la DCB? En caso de inactividad, ¿qué otras opciones tienen los usuarios para tener el servicio?

18. Medios de almacenamiento de la información y si cuenta con algún método de protección para los mismos
19. ¿Se realizan respaldos? En caso afirmativo, indicar periodicidad, cómo se realiza y si se tiene algún proceso de verificación de éstos
20. ¿Se tiene actualmente algún plan de contingencia en caso de alguna anomalía en el servidor? En caso afirmativo, explíquelo brevemente
21. ¿Se cuenta con un historial de incidentes de seguridad y sus resoluciones?

22. ¿Cómo se realiza la transferencia de archivos de manera remota? (en caso de que aplique, ejemplo: telnet, ssh, etc…)
23. Usuarios y grupos válidos (tanto normales, como de administración)

Grupo	Privilegios

Usuario	Grupo	Privilegios adicionales a los del grupo

24. ¿Cómo se autentica un usuario en el servidor?
25. ¿Cuenta con una política de actualizaciones? En caso afirmativo, indicarla
26. ¿Cuenta con una política de contraseñas? En caso afirmativo indicarla
27. Liste los controles de seguridad que se ocupan en el servidor y explíquelos
28. Describa brevemente el funcionamiento de los servicios que se ofrecen en el servidor
29. Indique el equipo activo (hubs, switches, ruteadores, access points, etc...) que se tiene en su área . Mencione marca, modelo y velocidades que maneja
30. Indique el esquema del equipo activo de su área (si están cascadeados, apilados, si se conectan a equipos activos de otras áreas, etc...)
31. ¿El equipo activo cuenta con algún tipo de control de seguridad física? En caso afirmativo, indicarlo
32. ¿Quién es el personal que tiene acceso al equipo activo?
33. Aproximadamente, ¿a cuántos nodos da servicio el equipo activo de su área?
34. ¿Los switches con los que se cuenta, son administrables? En caso afirmativo, indicar el método por el cual se administran (puerto de consola, telnet, ssh, web, etc...)
35. ¿El equipo activo tiene las contraseñas por default, o ya han sido cambiadas?
36. ¿Se han creado VPN´s en el equipo activo? (VPN: una red privada que utiliza Internet como medio de transporte, pero que mantiene la seguridad de la información que viaja a través de ésta)
37. Indique los parámetros que se han administrado en el equipo activo de su área
38. En caso de tener algún Access Point en su área, mencione quiénes pueden conectarse a través de éste
39. ¿Qué requiere un usuario para poder conectarse al Access Point de su área? (documentación, autorización, etc...)
40. Indique el tipo de seguridad que maneja el Access Point de su área (ninguna, WEP, WPA, etc...)
41. ¿Cuenta con una política de respaldo de las modificaciones que se hacen al equipo activo? En caso afirmativo, indicarla
42. ¿Se tiene algún plan de contingencia en caso de que falle el equipo activo de su área? En caso afirmativo, indicarlo

3.4 CUESTIONARIO PARA LA CARACTERIZACIÓN DE LAS APLICACIONES DE LA RED DE CÓMPUTO DE LA DCB DE LA UNAM

1. Nombre de la aplicación _____
2. Sistema operativo y versión sobre la que está montado _____
3. Versión del kernel (en caso de que aplique) _____
4. IP y alias del equipo donde esté montada la aplicación _____
5. ¿Bajo qué lenguaje la aplicación fue desarrollada y con qué herramienta fue compilado (mencione la versión)?
6. ¿Por qué medio se accede a la aplicación? Indique versiones. (ejemplo: web, Apache 2.2.10)
7. Describa brevemente qué funciones realiza el sistema
8. ¿El equipo donde está montada la aplicación, cuenta con alguna medida de seguridad física para su acceso? En caso afirmativo, indique cuál
9. Requerimientos de disponibilidad de la aplicación

(disponibilidad: propiedad de ser accessible y utilizable a petición por entidades autorizadas)

- □ Siempre disponible
- □ Días y horas hábiles
- □ Otro : _____

10. Requerimientos de disponibilidad de la información que maneja la aplicación
    - □ Siempre disponible
    - □ Días y horas hábiles
    - □ Otro : _____
11. Requerimientos de integridad de la información que maneja la aplicación (integridad: propiedad de la información que asegura que ésta no ha sido alterada o destruida de manera no autorizada)

Seleccione una:

- □ Crítica
- □ Alta
- □ Media
- □ Baja

12. Requerimientos de confidencialidad de la información que maneja la aplicación (confidencialidad: propiedad de la información que asegura que ésta no se encuentra disponible o es divulgada hacia individuos, entidades o procesos no autorizados)

Seleccione una o varias:

- Información Confidencial
- Información Interna
- Información Pública

13. Tipo de información que maneja la aplicación
14. Información que se genera (de salida), requiere (de entrada), se procesa y es almacenada por la aplicación
15. Importancia de la información que maneja la aplicación para la DCB
16. ¿Qué información manejada por la aplicación o a punto de ser manejada por ésta no debe ser divulgada y a quiénes?
17. Explique cuál es el impacto potencial a la DCB si la información es divulgada a personal no autorizado
18. ¿Qué valor le asignaría a la información que maneja la aplicación?

Seleccione una:

- Valor Crítico
- Valor Alto
- Valor Medio
- Valor Bajo

19. Medios de almacenamiento de la información y si cuenta con algún método de protección para los mismos
20. ¿Cuánto tiempo de inactividad del sistema se puede tolerar en la DCB? En caso de inactividad, ¿qué otras opciones tienen los usuarios para tener el servicio?
21. ¿Cuál es el efecto que causaría en la DCB si la aplicación no es fiable?
22. ¿Se realizan respaldos? En caso afirmativo, indicar periodicidad, cómo se realiza y si se tiene algún proceso de verificación de éstos
23. ¿Se tiene actualmente algún plan de contingencia en caso de alguna anomalía en la aplicación? En caso afirmativo, explíquelo brevemente
24. ¿Se cuenta con un historial de incidentes de seguridad y sus resoluciones?
25. ¿Cómo se realiza la transferencia de archivos de manera remota? (en caso de que aplique, ejemplo: telnet, ssh, etc…)

26. Usuarios y grupos válidos (tanto normales, como de administración)

Grupo	Privilegios

Usuario	Grupo	Privilegios adicionales a los del grupo

27. ¿Cómo se autentica un usuario la aplicación?
28. ¿Cuenta con una política de actualizaciones? En caso afirmativo, indicarla
29. ¿Cuenta con una política de contraseñas? En caso afirmativo indicarla
30. Liste los controles de seguridad que se utilizan en la aplicación y explíquelos

3.5 DOCUMENTACIÓN DE LAS ACTIVIDADES DEL ANÁLISIS DE RIESGOS

- **I. Introducción**

El proceso de análisis de riesgos busca identificar y valorar los posibles riesgos que, en caso de que se presenten, podrían tener un impacto negativo en la misión de la DCB.

Tiene como alcance los activos de cómputo dentro de la División, tanto los equipos como el personal.

- **II. Enfoque del Análisis de Riesgos**

Se determinó realizar un análisis de riesgos cualitativo, ya que es un poco más eficiente en cuanto a tiempo, además de que no se cuentan con valores monetarios para la información valiosa de la DCB.

Se determinó realizar cuestionarios y entrevistas a los responsables y administradores de equipo de cómputo sensible, además de entrevistas a usuarios normales de los servicios de cómputo que ofrece la División.

También se hizo una búsqueda en Internet en sitios de reputación conocida como el US-CERT (United States-Computer Emergency Readiness Team), CVE (Common Vulnerabilities and Exposures), NIST-NVD (National Institute of Standards and Technology-National Vulnerability Database), SANS Internet Storm Center, Computer Security Vulnerabilities, y blogs de seguridad de Microsoft para identificar vulnerabilidades publicadas que puedan llegar a afectar a la División, así como el uso de herramientas automatizadas para la identificación de éstas, como Nessus 4, Acunetix XSS Scanner y Nikto Web Server Scanner, además de un reporte elaborado por la compañía Qualys, mediante el Qualys FreeScan Vulnerabilities Report.

- **III. Caracterización del Sistema**

- Hardware

    - Aproximadamente 350 equipos de cómputo (PC´s y laptops). Del cual aproximadamente una cuarta parte cuenta con procesadores obsoletos como Pentium Celeron, Pentium II, Pentium III y anteriores; el equipo restante tiene procesadores Pentium D, Core Duo, Core 2 Duo y equivalentes. La gran mayoría tiene como sistema operativo Windows XP SP3

- 5 servidores con procesadores de alto rendimiento. Todos corriendo en Linux como sistema operativo
- Alrededor de 50 impresoras, cuyos modelos varían desde los de inyección de tinta, los multifuncionales, hasta los de impresión a grandes volúmenes a color
- Cerca de 30 proyectores
- 19 pizarrones electrónicos
- 17 dispositivos de conexión de redes, entre hubs, switches y access points
- 1 cámara digital
- Alrededor de 135 equipos supresores de picos y no-breaks
- Grán número de memorias USB

- Software

  - Matemático (Matlab, Matematica, Maple, MathType, Geogebra, Descartes, MathCAD)
  - Ofimático (MS Office 2000, 2003 y 2007, OpenOffice)
  - Dibujo (AutoCad 2000,2004, 2007, Corel Draw, ChemLab, PSPICE)
  - Edición de Archivos (Adobe Acrobat, Photoshop)
  - Para lecturas ópticas (Pearson NCS ScanToolsPlus)
  - Antivirus (Kaspersky, Avira, McAfee, Norton)
  - Estadístico (SPSS, Statistica)
  - Bases de Datos (MySQL, PostgreSQL)
  - Mensajería (MSN Messenger, Skype)
  - Didáctico (Second Life)
  - Conectividad (SSH Secure Shell)
  - Grabadores de CD y DVD (Nero, Roxio)

- Tipos de información manejada

  - Académica
  - Administrativa
  - Administración de redes
  - Personal (nombre, dirección, teléfonos, etc...)
  - Configuraciones de servicios
  - Datos de sesiones de prácticas de laboratorio.

- Personal que utiliza y mantiene los sistemas de TI

    - Personal de la Coordinación de Cómputo de la DCB y de algunas coordinaciones.

- Nivel crítico de los Servidores y Aplicaciones

    - Servidores (por razones de seguridad no se mencionan nombres):
        - 5 servidores con nivel crítico alta
    - Aplicaciones (Aplicación-Nivel de Nivel crítico):
        - Sistema Integral de Información de la DCB (SII-DCB) – Alta
        - Base de Datos del Sistema Integral de Información de la DCB (SII-DCB) – Alta
        - Sistema de gestión de Información del Personal Académico de la DCB (SIGECI-DCB) –Alta
        - Sistema de Información de Actividades Académicas de la DCB (SIAA-DCB) –Alta
        - Control de Correspondencia –Alta
        - Registro de usuarios del TCA – Bajo
        - Prácticas de Mecánica – Bajo

- Sensibilidad de los Servidores y Aplicaciones

    - Servidores:
        - 3 servidores con sensibilidad alta
        - 2 servidores con sensibilidad media
    - Aplicaciones (Aplicación-Nivel de Sensibilidad):
        - Sistema Integral de Información de la DCB (SII-DCB) – Alta
        - Base de Datos del Sistema Integral de Información de la DCB (SII-DCB) – Alta
        - Sistema de gestión de Información del Personal Académico de la DCB (SIGECI-DCB) –Media
        - Sistema de Información de Actividades Académicas de la DCB (SIAA-DCB) –Alta
        - Control de Correspondencia –Media
        - Registro de usuarios del TCA – Baja
        - Prácticas de Mecánica – Bajo

- Grupos y Usuarios

    - Existe un gran número de grupos en los distintos servidores y aplicaciones de la DCB, van desde grupos de administración, grupos con mínimos privilegios, y grupos con diversos privilegios como de consulta, captura, monitoreo, actualización, entre otros.

- Políticas de Seguridad que rigen a la DCB

    - Políticas de Seguridad de la FI
    - Políticas de Seguridad de la DCB (en proceso)

- Protección de Medios de Almacenamiento de la Información

    - En general, no se cuenta en ningún área con una protección de medios de almacenamiento.

- Entorno de Seguridad Física de los Sistemas de TI

    - Los equipos cuentan con un resguardo, donde se indica quién es el responsable.
    - La gran mayoría sólo se encuentra asegurado de la misma manera que se aseguran los cubículos, únicamente con llave.
    - Los equipos ubicados en los salones se encuentran resguardados mediante puertas con cerradura electrónica que hace uso de biometría y control de acceso, además cuentan con alarmas de seguridad.

- **IV. Resultados**

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
1	Ciertos equipos escuchan en el puerto 137 y contestan a peticiones NetBIOS nbtscan	Usuarios no autorizados	Obtención de nombres de sistema y de dominio	Bajo	10.6.1 Controles de red
2	Obtención de información de sistema operativo de distintos equipos de la red de la DCB	Usuarios no autorizados	Utilización de distintas herramientas de auditoría	Bajo	10.6.1 Controles de red
3	Ciertos equipos cuentan con los protocolos CIFS o SMB, utilizados para compartir archivos, carpetas o impresoras dentro de nodos en una red	Usuarios no autorizados	Enumeración de carpetas compartidas dentro de los distintos hosts de la red de la DCB	Medio	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
4	Es posible el acceso a distintos equipos mediante sesiones nulas y/o cuentas de invitado	Usuarios no autorizados	Acceso no autorizado a los equipos	Bajo	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
5	Ciertos equipos responden a peticiones SMB para la obtención del host SID	Usuarios no autorizados	Enumeración de usuarios locales	Bajo	10.6.1 Controles de red
6	Es posible acceder a ciertos equipos mediante usuarios invitados, utilizando cuentas aleatorias	Usuarios no autorizados	Acceso no autorizado a los equipos	Bajo	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
7	Ciertos equipos tienen una o más carpetas compartidas de Windows. Dependiendo de los privilegios de dichas carpetas es posible la lectura/escritura remotamente	Usuarios no autorizados	Acceso no autorizado a carpetas compartidas. Modificación a destrucción de información. Alteración de la integridad	Medio	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
8	Ciertos equipos permiten el acceso al Registro de Windows mediante ciertas combinaciones de login / contraseña	Usuarios no autorizados	Acceso no autorizado al registro de Windows	Bajo	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
9	Mediante ciertas herramientas, es posible identificar archivos compartidos de Office	Usuarios no autorizados	Enumeración de archivos compartidos	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
10	Posibles conexiones al puerto 1031 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC	Bajo	10.6.1 Controles de red
11	Posibles conexiones al puerto 2103 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC	Bajo	10.6.1 Controles de red
12	Posibles conexiones al puerto 1026 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC	Bajo	10.6.1 Controles de red
13	Posibles conexiones al puerto 2107 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC	Bajo	10.6.1 Controles de red
14	Posibles conexiones al puerto 2105 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC	Bajo	10.6.1 Controles de red
15	Posibles conexiones al puerto 135 tcp	Usuarios no autorizados	Enumeración y/o acceso a servicios DCERPC	Bajo	10.6.1 Controles de red
16	Utilización de herramientas para la identificación del tipo y versión de servidores web	Usuarios no autorizados	Obtención de información de servidores web	Medio	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
17	Los métodos TRACK y TRACE están habilitados en ciertos equipos con servidores web. Son vulnerables a ataques XST (Cross Site Tracking), que pueden ser usados para la obtención sin	Usuarios no autorizados	Obtención de credenciales de usuarios mediante XST	Medio	5.1.1 Documento de política de seguridad de la información 11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	autorización de credenciales				10.6.1 Controles de red
18	Es posible la detección de servidores VMWare en ciertos equipos mediante peticiones al puerto 912	Usuarios no autorizados	Mapeo de redes	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
19	Es posible la detección de servidores web mediante peticiones a los puertos 80 y 443	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
20	Ciertos equipos cuentan con certificados SSL expirados o a expirar prontamente, relacionados a servicios	Usuarios no autorizados	Falla en autenticación	Bajo	10.6.1 Controles de red
21	Ciertos equipos cuentan con protocolos de cifrado de tráfico de red como SSL anticuados (SSLv2)	Usuarios no autorizados	Explotación de vulnerabilidades conocidas en SSL v2	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
22	Ciertos equipos que utilizan SSL hacen uso de protocolos que realizan cifrados débiles	Usuarios no autorizados	Pérdida de confidencialidad	Bajo	10.6.1 Controles de red
23	Ciertos equipos son vulnerables a desbordamiento de buffer, que permite ejecutar código arbitrario con los privilegios del sistema	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
24	Ciertos equipos cuentan con vulnerabilidades en SMB de corrupción de memoria, que permiten la ejecución de código arbitrario o una denegación de servicio	Usuarios no autorizados	DoS o ejecución de código arbitrario	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
25	Ciertos equipos Windows contienen una falla en el servicio de Cliente de Web	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
26	Ciertos equipos Windows contienen una falla en el	Usuarios no autorizados	Ejecución de código arbitrario desde hosts	Bajo	11.4.2 Autenticación de usuarios para

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	servicio de cola de impresión		remotos		conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
27	Ciertos equipos Windows contienen una falla en la implementación SMB	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
28	Ciertos equipos Windows contienen una versión del protocolo SMB (SMBv2), que cuenta con una serie de vulnerabilidades que permiten la ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
29	Ciertos equipos Windows contienen una falla en la intefaz RPC que permite ejecución de código arbitrario y/o lograr privilegios del Sistema	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
30	Ciertos equipos cuentan con servidores web que hacen uso de versiones de PHP obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	Acceso no autorizado, DoS y ejecución de código arbitrario	Medio	11.4.1 Política sobre el uso de servicios de red
					10.6.1 Controles de red
31	Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	DoS y XSS	Medio	11.4.1 Política sobre el uso de servicios de red
					11.4.2 Autenticación de usuarios para conexiones externas
					10.6.1 Controles de red
32	Ciertos equipos hacen uso de la distribución	Usuarios no autorizados	Ejecución de código arbitrario desde hosts	Bajo	11.4.1 Política sobre el uso de servicios de red

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de desbordamiento de buffer		remotos		11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
33	Es posible la detección de equipos con servicios SMTP activos	Usuarios no autorizados	Envío de spam a través de equipos de la red	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
34	Ciertos equipos que manejan el protocolo SNMP cuentan con los nombres de comunidades por default (private y public)	Usuarios no autorizados	Cambios no autorizados en configuraciones de equipos	Bajo	11.3.1 Uso de contraseñas 11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
35	Ciertos equipos son vulnerables a ataques de Etherleak (cuando una NIC rellena las tramas con información de paquetes anteriores o con información de la memoria del kernel, en lugar de con bytes nulos)	Usuarios no autorizados	Pérdida de confidencialidad	Bajo	10.6.1 Controles de red
36	Ciertos equipos reportan las versiones de los servidores web utilizados mediante páginas de error	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Medio	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
37	Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache Tomcat obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Usuarios no autorizados	XSS	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
38	Es posible la obtención de información de servidores web mediante peticiones al puerto 5353 udp	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
39	Es posible la obtención de información de	Usuarios no autorizados	Mapeo de redes e identificación de	Bajo	11.4.1 Política sobre el uso de servicios de red

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	servidores DNS		objetivos		10.6.1 Controles de red
40	Un servidor DNS responde a cualquier petición	Usuarios no autorizados	DDoS	Bajo	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
41	Posible identificación de cuentas y servicios mediante el servicio ident (auth)	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
42	Es posible la obtención de información de servidores SSH	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
43	Ciertos equipos que cuentan con el servicio SSH habilitado son vulnerables a ataques de secuestro de sesiones X11	Usuarios no autorizados	Autenticación errónea y/o pérdida de confidencialidad	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
44	Ciertos servidores cuentan con versiones de SO obsoletas	Usuarios no autorizados	Pérdida de confidencialidad,, integridad, autenticación y disponibilidad	Bajo	10.3.1 Gestión de la Capacidad
45	En ciertos equipos Windows que cuentan con un servidor de protocolo de escritorio remoto, son vulnerables a ataques de hombre en medio	Usuarios no autorizados	Acceso no autorizado	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
46	Ciertos equipos Wndows cuentan con el servicio de terminales remotas, que es propenso a ataques de hombre en medio	Usuarios no autorizados	Acceso no autorizado	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
47	Ciertos equipos con el servicio SSH, cuentan con una versión insegura del protocolo (SSHv1)	Usuarios no autorizados	Pérdida de confidencialidad	Bajo	10.6.1 Controles de red
48	Ciertos equipos con el servicio Samba	Usuarios no autorizados	Ejecución de código arbitrario desde hosts	Bajo	11.4.2 Autenticación de usuarios para

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	habilitado, cuentan con una versión obsoleta que es vulnerable a desbordamientos de buffer remotos cuando recibe un paquete malicioso SMB		remotos		conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
49	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que permite a un atacante el acceso a archivos arbitrarios fuera de las rutas compartidas permitidas	Usuarios no autorizados	Acceso no autorizado	Medio	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
50	Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que, al momento de recibir una petición FindNextPrintChangeNotify() sin haber recibido previamente una llamada FindFirstPrintChangeNoticy() puede ocasionar un DoS	Usuarios no autorizados	DoS	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
51	Ciertos equipos con el servicio FTP habilitado, permiten que las credenciales de los usuarios sean transmitidas en claro	Usuarios no autorizados	Autenticación errónea y/o pérdida de confidencialidad	Bajo	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
52	En ciertos equipos es posible montar volúmenes NFS sin contar con privilegios de root	Usuarios no autorizados	Acceso no autorizado	Bajo	11.4.1 Política sobre el uso de servicios de red 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
53	En ciertos equipos con el protocolo FTP habilitado, se permiten accesos anónimos	Usuarios no autorizados	Pérdida de confidencialidad	Medio	11.4.1 Política sobre el uso de servicios de red 10.6.1 Controles de red
54	Algunos servidores web son vulnerables a	Usuarios no autorizados	Pérdida de confidencialidad	Medio	11.4.2 Autenticación de usuarios para

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	ataques de directorio transversal				conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
55	En ciertos equipos es posible listar el software instalado mediante SNMP	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	11.4.1 Política sobre el uso de servicios de red
					10.6.1 Controles de red
56	Ciertos equipos tienen instalado Common Management Agent, un componente del manejador de seguridad del sistema de McAfee. Éste contienen una serie de vulnerabilidades que pueden permitir a un atacante causar un DoS, lanzar un ataque de directorio transversal y/o ejecutar código arbitrario	Usuarios no autorizados	DoS, acceso no autorizado y ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
57	Ciertos equipos Windows cuentan con versiones del Task Scheduler vulnerables a la ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
58	Ciertos equipos tienen como sistema operativo versiones de MS Windows (Windows 95 / 98 / Me)que ya no son mantenidas por Microsoft, por lo que ya no son publicados parches de seguridad para éstas.	Usuarios no autorizados	Explotación de múltiples vulnerabilidades	Bajo	10.3.1 Gestión de la Capacidad
59	Ciertos equipos tienen habilitada la opción de SMTP relay	Usuarios no autorizados	Envío de spam a través de equipos de la red y posible DoS en la red	Bajo	11.4.1 Política sobre el uso de servicios de red
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
60	Es posible la	Usuarios no	Mapeo de redes e	Bajo	11.4.1 Política sobre el

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	identificación de versiones de los servidores SQL en Windows	autorizados	identificación de objetivos		uso de servicios de red 10.6.1 Controles de red
61	Ciertos equipos responden a peticiones WMI (Windows Management Instrumentation)	Usuarios no autorizados	Mapeo de redes, identificación de objetivos, obtención de credenciales y configuraciónes de red	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
62	Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos y DoS	Bajo	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
63	Ciertos equipos Windows, cuentan con versiones del servicio Plug and Play que permite la ejecución de código arbitrario y elevación de privilegios	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
64	Es posible la lectura de las bitácoras de eventos en equipos con Windows 2000	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	10.3.1 Gestión de la Capacidad 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
65	Es posible la enumeración de los servicios que se encuentran activos en equipos Wndows 2000, a través de sesiones nulas	Usuarios no autorizados	Mapeo de redes e identificación de objetivos	Bajo	10.3.1 Gestión de la Capacidad 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
66	Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	del Sistema				recursos del sistema
					10.6.1 Controles de red
67	Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	10.3.1 Gestión de la Capacidad
					11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
68	Existen equipos con servidores web vulnerables a ataques de directorio transversal	Usuarios no autorizados	Acceso no autorizado	Medio	11.4.2 Autenticación de usuarios para conexiones externas
					11.5.4 Uso de los recursos del sistema
					10.6.1 Controles de red
69	Ciertos equipos tienen habilitado el servicio de telnet	Usuarios no autorizados	Pérdida de confidencialidad	Medio	11.4.1 Política sobre el uso de servicios de red
					10.6.1 Controles de red
70	Ciertos equipos tienen instalada una versión de MathCad (12, 13 y 13.1) que es vulnerable a cambios de contraseñas en archivos protegidos, remoción completa de protecciones y acceso a información.	Usuarios no autorizados	Acceso no autorizado a archivos protegidos	Bajo	10.3.1 Gestión de la Capacidad
71	En la gran mayoría de equipos se tienen instaladas versiones de MS Office que no son actualizadas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Usuarios no autorizados	Pérdida de confidencialidad, integridad, autenticación, y acceso no autorizado.	Medio	10.3.1 Gestión de la Capacidad
72	En ciertos equipos se tienen instaladas versiones de Open Office que son obsoletas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Usuarios no autorizados	Pérdida de confidencialidad, integridad, autenticación, y acceso no autorizado.	Bajo	10.3.1 Gestión de la Capacidad

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
73	En ciertos equipos se tienen instaladas versiones de Autocad (2005 y 2006) que cuenta con una vulnerabilidad no divulgada que permite a un atacante obtener privilegios elevados	Usuarios no autorizados	Acceso no autorizado	Bajo	10.3.1 Gestión de la Capacidad
74	La mayoría de los equipos tienen instaladas versiones obsoletas de Adobe Acrobat que cuentan con vuln. conocidas	Usuarios no autorizados	Pérdida de confidencialidad, integridad, autenticación, y acceso no autorizado.	Medio	10.3.1 Gestión de la Capacidad 10.6.1 Controles de red
75	La gran mayoría de los equipos cuentan con una versión de Kaspersky Antivirus (2008), que cuenta con una vulnerabilidad que permite a un usuario local, obtener privilegios del sistema	Usuarios no autorizados	Elevación de privilegios	Bajo	10.3.1 Gestión de la Capacidad 10.6.1 Controles de red
76	En ciertos equipos se encuentra instalado Avira Antivir, que cuenta con una vulnerabilidad que permite la elevación de privilegios.	Usuarios no autorizados	Elevación de privilegios	Bajo	10.3.1 Gestión de la Capacidad 11.5.4 Uso de los recursos del sistema
77	Ciertos equipos cuentan McAfee Antivirus que cuenta con vulnerabilidades que permiten a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, DoS	Bajo	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
78	Ciertos equipos cuentan con Norton Antivirus, que cuenta con vulnerabilidades permiten a la ejecución de código arbitrario y/o DoS	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, DoS	Bajo	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
79	En ciertos equipos se tienen instaladas	Usuarios no autorizados	Ejecución de código arbitrario desde hosts	Bajo	10.3.1 Gestión de la Capacidad

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	versiones de MySQL que cuentan con una serie de vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado		remotos, DoS, pérdida de integridad, elevación de privilegios, acceso no autorizado		11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
80	En ciertos equipos se tienen instaladas versiones de MSN Live Messenger, que son vulnerables a ataques DoS del servicio	Usuarios no autorizados	DoS	Medio	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
81	En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción de datos	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, pérdida de integridad	Bajo	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
82	En ciertos equipos se tienen instalada una versión de Nero Media Player, que es vulnerable a DoS de la aplicación	Usuarios no autorizados	DoS	Bajo	10.3.1 Gestión de la Capacidad 11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
83	Ciertos equipos cuentan con versiones de Samba (2.2.7) que son vulnerables a ataques de directorio transversal	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, acceso no autorizado, DoS	Bajo	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	que permiten acceder a directorios protegidos, DoS, ejecución de código arbitrario.				10.6.1 Controles de red
84	Ciertos equipos cuentan con versiones de Samba (3.0.3) que son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos, acceso no autorizado, DoS	Bajo	11.4.1 Política sobre el uso de servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 11.5.4 Uso de los recursos del sistema 10.6.1 Controles de red
85	Ciertos equipos cuentan con una versión de Apache Tomcat (5.5.26) que es vulnerable a ataques XSS	Usuarios no autorizados	XSS	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
86	Ciertos equipos cuentan con una versión de Subversion (1.5.1) que es vulnerable a ejecución de código arbitrario	Usuarios no autorizados	Ejecución de código arbitrario desde hosts remotos	Bajo	11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
87	Ciertos equipos cuentan con una versión del proxy Squid (2.5) que es vulnerable a ataques Dos, suplantación de IP, accesos no autorizados y divulgación de información no autorizada	Usuarios no autorizados	DoS, suplantación de IP, acceso no autorizado y pérdida de confidencialidad	Medio	11.4.2 Autenticación de usuarios para conexiones externas 10.6.1 Controles de red
88	No se cuenta con una Misión de Seguridad en la DCB	Usuarios autorizados y no autorizados	Violación a la normatividad no formalmente establecida	Alto	5.1.1 Documento de política de seguridad de la información
89	Ciertos funcionarios con altos privilegios a los recursos de la red cuentan con contraseñas débiles	Usuarios autorizados y no autorizados	Se pueden comprometer las credenciales de personal con altos privilegios dentro de la red de la DCB	Medio	5.1.1 Documento de política de seguridad de la información 11.3.1 Uso de contraseñas

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
90	No se cuenta con la debida asignación de responsabilidades en seguridad informática	Usuarios autorizados	Deslinde de responsabilidades	Medio	5.1.1 Documento de política de seguridad de la información 6.1.3 Asignación de responsabilidades relativas a las seguridad de la información
91	Ciertos equipos de funcionarios de la DCB no cuentan con controles de acceso para restringir privilegios a ayudantes	Usuarios autorizados	Acceso no autorizado, pérdida de confidencialidad e integridad	Medio	5.1.1 Documento de política de seguridad de la información 11.5.1 Procedimientos seguros de inicio de sesión 11.5.2 Identificación y autenticación de usuario
92	En el caso de las políticas de seguridad de la Facultad de Ingeniería, no son conocidas por los usuarios de la DCB	Usuarios autorizados	No cumplimiento de las políticas de seguridad que rigen a la FI	Alto	5.1.1 Documento de política de seguridad de la información
93	No se cuentan con políticas escritas de respaldos de información, protección y verificación de éstos	Usuarios autorizados	Pérdida de información en caso de incidentes	Medio	5.1.1 Documento de política de seguridad de la información 10.5.1 Copias de seguridad de la información 10.7.1 Gestión de medios removibles 10.7.3 Procedimientos de manipulación de la información
94	No se cuentan con políticas escritas de protección a medios de almacenamiento	Usuarios autorizados	Pérdida de confidencialidad e integridad	Medio	5.1.1 Documento de política de seguridad de la información 10.7.1 Gestión de medios removibles 10.7.3 Procedimientos de manipulación de la información 11.1.1 Políticas de control de acceso
95	En ciertos servidores y aplicaciones no se lleva un historial de incidentes de seguridad y sus resoluciones	Usuarios autorizados	Posible repetición de un mismo incidente sin que se tomen medidas para evitarlo	Bajo	5.1.1 Documento de política de seguridad de la información 10.10.1 Registro de auditoría 13.2.2 Aprendizaje de los incidentes de

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
					seguridad de la información
96	No se cuentan con políticas escritas de contraseñas	Usuarios autorizados	Pérdida de confidencialidad, integridad y acceso no autorizado	Alto	5.1.1 Documento de política de seguridad de la información 11.3.1 Uso de contraseñas
97	No se cuentan con políticas escritas de actualizaciones a sistemas y aplicaciones	Usuarios autorizados	Exposición a vulnerabilidades	Alto	5.1.1 Documento de política de seguridad de la información
98	Cualquier usuario puede instalar aplicaciones en los equipos a los que tienen acceso	Usuarios autorizados	Instalación de software malicioso, no actualizado o con vulnerabilidades conocidas	Medio	5.1.1 Documento de política de seguridad de la información 10.10.2 Supervisión del uso de sistema
99	No se cuenta con control alguno respecto a las aplicaciones que pueden ser instaladas o no en los equipos de la DCB dentro de las áreas de coordinaciones, secciones académicas, laboratorios y cubículos en general.	Usuarios autorizados	Instalación de software malicioso, no actualizado o con vulnerabilidades conocidas	Medio	5.1.1 Documento de política de seguridad de la información 10.10.2 Supervisión del uso de sistema 10.4.1 Controles contra el código malicioso
100	Existen equipos con información valiosa para la DCB que cuentan con IPs reales, por lo que podrían ser accedidos desde fuera de la red de la División	Usuarios autorizados	Exposición de equipos críticos a redes públicas	Alto	5.1.1 Documento de política de seguridad de la información 10.6.1 Controles de red
101	No se realiza un monitoreo adecuado del tráfico en la red de la DCB	Usuarios autorizados	Posibles intrusiones	Medio	10.6.1 Controles de red

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
102	En ciertos servidores y aplicaciones, el único control de acceso existente es por medio de nombre de usuario y contraseña	Usuarios autorizados	Acceso no autorizado en caso de que las credenciales se vean comprometidas	Medio	11.3.1 Uso de contraseñas
103	No se cuenta con un correcto inventario de activos informáticos	Usuarios autorizados	Pérdida de activos informáticos	Bajo	7.1.1 Inventario de activos 7.1.2 Propiedad de los activos
104	No se cuenta con una política de uso aceptable de los recursos informáticos y las sanciones en caso de violar éste a nivel de la DCB	Usuarios autorizados	Mal uso de los recursos informáticos	Alto	5.1.1 Documento de política de seguridad de la información 7.1.3 Uso aceptable de los activos
105	El equipo activo de la DCB cuenta con las contraseñas por default en usuarios privilegiados	Usuarios autorizados	Acceso no autorizado	Bajo	5.1.1 Documento de política de seguridad de la información 11.3.1 Uso de contraseñas
106	No se cuenta con una clasificación de los recursos informáticos, con base en su nivel crítico y/o sensibilidad	Usuarios autorizados	Pérdida de disponibilidad y/o confidencialidad	Medio	7.2.1 Directrices de clasificación 7.2.2 Etiquetado y manipulación de la información
107	No se cuenta con una capacitación de seguridad adecuada a la mayoría de los usuarios	Usuarios autorizados	Uso indebido de activos, exposición a vulnerabilidades, incumplimiento de políticas	Alto	5.1.1 Documento de política de seguridad de la información 8.2.2 Concienciación, formación y capacitación en seguridad de la información
108	No se cuentan con procedimientos de terminación de empleados o cambios de éstos (baja de claves, contraseñas, devolución de activos, privilegios, etc…)	Usuarios autorizados	Acceso no autorizado	Medio	8.3.1 Responsabilidad del cese o cambio 8.3.2 Devolución de activos 8.3.3 Retiro de los derechos de acceso

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
109	No se cuenta con equipo específicamente destinado a desarrollo y/o pruebas	Usuarios autorizados	Poner en riesgo los servicios ofrecidos	Medio	10.1.4 Segregación de los recursos de desarrollo, prueba y operación
110	No se cuentan con políticas de gestión de privilegios y revisión periódica de los mismos	Usuarios autorizados	Acceso no autorizado, pérdida de confidencialidad e integridad	Bajo	5.1.1 Documento de política de seguridad de la información 11.1.1 Políticas de control de acceso
111	No se cuentan con políticas documentadas sobre el uso de los servicios de la red	Usuarios autorizados	Uso indebido de los servicios de la red	Medio	5.1.1 Documento de política de seguridad de la información 7.1.3 Uso aceptable de los activos 11.4.1 Política sobre el uso de servicios de red
112	No se cuenta con un control adecuado establecido de conexión de equipos personales a la red	Usuarios autorizados	Acceso no autorizado	Medio	5.1.1 Documento de política de seguridad de la información 11.4.6 Control de la conexión a la red
113	Los equipos críticos o sensibles de la DCB no se encuentran debidamente segregados	Usuarios autorizados	Acceso no autorizado, DoS, exposición a diversas vulnerabilidades	Medio	11.4.5 Segregación de las redes
114	No se cuenta con una política escrita de requerimientos mínimos para el acceso a los servicios de la red	Usuarios autorizados	Exposición a vulnerabilidades	Medio	5.1.1 Documento de política de seguridad de la información 10.3.1 Gestión de la Capacidad 10.3.2 Aceptación del sistema
115	La información valiosa para la DCB no es almacenada de forma cifrada	Usuarios autorizados	Pérdida de confidencialidad	Medio	10.8.1 Políticas y procedimientos de intercambio de información
116	No se cuenta con una debida gestión sobre avisos de vulnerabilidades técnicas que afecten al equipo de la DCB ni los procedimientos de apilcación	Usuarios autorizados	Exposición a vulnerabilidades de publicación reciente	Bajo	5.1.1 Documento de política de seguridad de la información
117	No se cuenta con procedimientos escritos en caso de incidentes de	Usuarios autorizados	Tardanza en la resolución del incidente	Medio	5.1.1 Documento de política de seguridad de la información

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
	seguridad				13.1.1 Notificación de los eventos de seguridad de la información
118	No se cuenta con una política de realización de estudios de gestión de riesgos	Usuarios autorizados	No hay identificación, mitigación o aceptación de riesgos	Bajo	5.1.1 Documento de política de seguridad de la información 14.1.2 Continuidad del negocio y evaluación de riesgos
119	En caso de falla en el suministro de electricidad prolongado, no hay opción alternativa para continuar con los servicios de la DCB	Falla en el suministro de electricidad	Pérdida de disponibilidad	Medio	9.2.2 Instalaciones de suministro
120	No existe documentación que indique los procedimientos a seguir en caso de aviso previo de falla en el suministro de electricidad	Falla en el suministro de electricidad	Posibles fallas en los servicios de la División	Medio	9.2.2 Instalaciones de suministro
121	No existe doc. que indique los proedi-mientos a seguir cuando se recupere el suministro de electricidad después de fallas	Falla en el suministro de electricidad	Posibles fallas en los servicios de la División	Medio	9.2.2 Instalaciones de suministro
122	No todos los equipos de la DCB cuentan con sistemas de regulación de voltaje y/o prevención en cortes de energía	Falla en el suministro de electricidad	Posibles fallas en los servicios y/o equipos de la División	Medio	9.2.2 Instalaciones de suministro
123	No existe documentación que indique los procedimientos a seguir antes y después de los periodos de vacaciones administrativas en la División	Usuarios autorizados	Posibles fallas en los servicios de la División	Medio	5.1.1 Documento de política de seguridad de la información
124	No existe documentación que indique los procedimientos a seguir antes y después de que ocurra un sismo	Terremotos	Posibles fallas en los servicios de la División	Bajo	9.1.4 Protecciones contra las amenazas externas y de origen ambiental

No.	Vulnerabilidad	Amenaza	Acción	Nivel de Riesgo	Recomendación de Controles
125	No existen procedimientos para el deshecho de documentación valiosa para la DCB	Usuarios no autorizados	Pérdida de confidencialidad	Medio	5.1.1 Documento de política de seguridad de la información
126	No hay control alguno para evitar la suplantación de IPs reales asignadas a la DCB	Usuarios no autorizados	Suplantación	Medio	10.6.1 Controles de red
127	Los profesores y alumnos comparten información por medio de dispositivos de almacenamiento como memorias flash, por los cuales se realiza la propagación de virus, spyware, caballos de troya, etc...	Usuarios no autorizados	Exposición a software malicioso	Medio	10.4.1 Controles contra el código malicioso

- **V. Resumen**

127 riesgos identificados totales

78 riesgos nivel Bajo

42 riesgos nivel Medio

7 riesgos nivel Alto

36 controles recomendados en total

3.6. DOCUMENTACIÓN DE LAS ACTIVIDADES DEL MANEJO DE RIESGOS

A continuación se muestra el programa propuesto para la implantación de los controles seleccionados.

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
Alta	Documento de política de seguridad de la información	No se cuenta con una Misión de Seguridad en la DCB	Alto	AR, RTCA, CC y JD	3 meses	Se deberá de elaborar el documento de las políticas de seguridad aplicables a la DCB.Se deberá de elaborar el documento de las políticas de seguridad aplicables a la DCB. Posteriormente éstas deberán de ser revisadas y actualizadas periódicamente. El documento deberá de ser aprobado por las autoridades de la DCB y acatado por toda la comunidad académica que la conforma, al igual que todo el personal externo que utilice los sistemas de información del área.
		Ciertos funcionarios con altos privilegios a los recursos de la red cuentan con contraseñas débiles	Medio			
		No se cuenta con la debida asignación de responsabilidades en seguridad informática	Medio			
		Ciertos equipos de funcionarios de la DCB no cuentan con controles de acceso para restringir privilegios a ayudantes	Medio			
		En el caso de las políticas de seguridad de la Facultad de Ingeniería, no son conocidas por los usuarios de la DCB	Alto			
		No se cuentan con políticas escritas de respaldos de información, protección y verificación de éstos	Medio			
		No se cuentan con políticas escritas de protección a medios de almacenamiento	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		En ciertos servidores y aplicaciones no se lleva un historial de incidentes de seguridad y sus resoluciones	Bajo			El documento de las Políticas de Seguridad deberá ser entregado a todo el personal de la DCB.
		No se cuentan con políticas escritas de contraseñas	Alto			
		No se cuentan con políticas escritas de actualizaciones a sistemas y aplicaciones	Alto			
		Cualquier usuario puede instalar aplicaciones en los equipos a los que tienen acceso	Medio			
		No se cuenta con control alguno respecto a las aplicaciones que pueden ser instaladas o no en los equipos de la DCB dentro de las áreas de coordinaciones, secciones académicas, laboratorios y cubículos en general.	Medio			
		Existen equipos con información valiosa para la DCB que cuentan con IPs reales, por lo que podrían ser accedidos desde fuera de la red de la División	Alto			
		No se cuenta con una política de uso aceptable de los recursos informáticos y las sanciones en caso de violar éste a nivel de la DCB	Alto			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		El equipo activo de la DCB cuenta con las contraseñas por default en usuarios privilegiados	Bajo			
		No se cuenta con una capacitación de seguridad adecuada a la mayoría de los usuarios	Alto			
		No se cuentan con políticas de gestión de privilegios y revisión periódica de los mismos	Bajo			
		No se cuentan con políticas documentadas sobre el uso de los servicios de la red	Medio			
		No se cuenta con un control adecuado establecido de conexión de equipos personales a la red	Medio			
		No se cuenta con una política escrita de requerimientos mínimos para el acceso a los servicios de la red	Medio			
		No se cuenta con una debida gestión sobre avisos de vulnerabilidades técnicas que afecten al equipo de la DCB ni los procedimientos de apilcación	Bajo			
		No se cuenta con procedimientos escritos en caso de incidentes de seguridad	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		No se cuenta con una política de realización de estudios de gestión de riesgos	Bajo			
		No existe documentación que indique los procedimientos a seguir antes y después de los periodos de vacaciones administrativas en la División	Medio			
		No existen procedimientos para el desecho de documentación valiosa para la DCB	Medio			
Alta	Uso aceptable de los activos	No se cuenta con una política de uso aceptable de los recursos informáticos y las sanciones en caso de violar éste a nivel de la DCB	Alto	CC, JD y CIPP	3 meses	Posteriormente éstas deberán de ser revisadas y actualizadas periódicamente. Se deberá de incluir dentro de las Políticas de Seguridad de la DCB.
		No se cuentan con políticas documentadas sobre el uso de los servicios de la red	Medio			
Alta	Concientización, formación y capacitación en seguridad de la información	No se cuenta con una capacitación de seguridad adecuada a la mayoría de los usuarios	Alto	RTCA	1 semana	Se deberá de realizar una campaña de concientización, para que todo el personal de la DCB tenga en cuenta la importancia de la seguridad en cómputo, posteriormente a la elaboración de las políticas de

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
						seguridad de la DCB, para que sean difundidas entre toda la comunidad de la DCB..
Alta	Política de control de acceso	No se cuentan con políticas escritas de protección a medios de almacenamiento	Medio	AR	3 meses	Se deberán crear listas de control de acceso para kos recursos que así lo requieran. Se debe incluir dentro de las políticas de seguridad.
		No se cuentan con políticas de gestión de privilegios y revisión periódica de los mismos	Bajo			
Alta	Uso de contraseñas	Ciertos equipos que manejan el protocolo SNMP cuentan con los nombres de comunidades por default (private y public)	Bajo	AR	3 meses	Deberán mantenerse confidenciales, no tenerlas en algún documento (en papel o digital), cambiarlas cuando se tenga l amenor sospecha de que hayan sido divulgadas, cambiarlas regularmente, que tengan una longitud igual o mayor a diez caracteres, que no estén basadas en información personal o en palabras de diccionario, no usar la misma contraseña para
		Ciertos funcionarios con altos privilegios a los recursos de la red cuentan con contraseñas débiles	Medio			
		No se cuentan con políticas escritas de contraseñas	Alto			
		En ciertos servidores y aplicaciones, el único control de acceso existente es por medio de nombre de usuario y contraseña	Medio			
		El equipo activo de la DCB cuenta con las contraseñas por default en usuarios privilegiados	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
						distintos propósitos y que no sean secuencias de números letras o números. Se debe incluir dentro de las políticas de seguridad.
Alta	Política sobre uso de los servicios de red	Ciertos equipos cuentan con los protocolos CIFS o SMB, utilizados para compartir archivos, carpetas o impresoras dentro de nodos en una red	Medio	AR	3 meses	Sólo se dará acceso a los servicios de la red al personal académico-administrativo que forma parte de la DCB. Deberán de establecerse normas para el otorgamiento y revocación de privilegios de dichos servicios. Se puede incluir dentro de las políticas de seguridad
		Es posible el acceso a distintos equipos mediante sesiones nulas y/o cuentas de invitado	Bajo			
		Es posible acceder a ciertos equipos mediante usuarios invitados, utilizando cuentas aleatorias	Bajo			
		Ciertos equipos tienen una o más carpetas compartidas de Windows. Dependiendo de los privilegios de dichas carpetas es posible la lectura/escritura remotamente	Medio			
		Ciertos equipos permiten el acceso al Registro de Windows mediante ciertas combinaciones de login / contraseña	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Mediante ciertas herramientas, es posible identificar archivos compartidos de Office	Bajo			
		Utilización de herramientas para la identificación del tipo y versión de servidores web	Medio			
		Los métodos TRACK y TRACE están habilitados en ciertos equipos con servidores web. Son vulnerables a ataques XST (Cross Site Tracking), que pueden ser usados para la obtención sin autorización de credenciales	Bajo			
		Es posible la detección de servidores VMWare en ciertos equipos mediante peticiones al puerto 912	Bajo			
		Es posible la detección de servidores web mediante peticiones a los puertos 80 y 443	Bajo			
		Ciertos equipos cuentan con protocolos de cifrado de tráfico de red como SSL anticuados (SSLv2)	Bajo			
		Ciertos equipos cuentan con vulnerabilidades en SMB de corrupción de memoria, que permiten la ejecución de código arbitrario o una denegación de servicio	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos cuentan con servidores web que hacen uso de versiones de PHP obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Medio			
		Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Medio			
		Ciertos equipos hacen uso de la distribución Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de desbordamiento de buffer	Bajo			
		Es posible la detección de equipos con servicios SMTP activos	Bajo			
		Ciertos equipos reportan las versiones de los servidores web utilizados mediante páginas de error	Medio			
		Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache Tomcat obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Bajo			
		Es posible la obtención de información de servidores web mediante peticiones al puerto 5353 udp	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Es posible la obtención de información de servidores DNS	Bajo			
		Un servidor DNS responde a cualquier petición	Bajo			
		Posible identificación de cuentas y servicios mediante el servicio ident (auth)	Bajo			
		Es posible la obtención de información de servidores SSH	Bajo			
		Ciertos equipos que cuentan con el servicio SSH habilitado son vulnerables a ataques de secuestro de sesiones X11	Bajo			
		Ciertos equipos con el servicio FTP habilitado, permiten que las credenciales de los usuarios sean transmitidas en claro	Bajo			
		En ciertos equipos es posible montar volúmenes NFS sin contar con privilegios de root	Bajo			
		En ciertos equipos con el protocolo FTP habilitado, se permiten accesos anónimos	Medio			
		En ciertos equipos es posible listar el software instalado mediante SNMP	Bajo			
		Ciertos equipos tienen habilitada la opción de SMTP relay	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Es posible la identificación de versiones de los servidores SQL en Windows	Bajo			
		Ciertos equipos tienen habilitado el servicio de telnet	Medio			
		Ciertos equipos cuentan con versiones de Samba (2.2.7) que son vulnerables a ataques de directorio transversal que permiten acceder a directorios protegidos, DoS, ejecución de código arbitrario.	Bajo			
		Ciertos equipos cuentan con versiones de Samba (3.0.3) que son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios	Bajo			
		No se cuentan con políticas documentadas sobre el uso de los servicios de la red	Medio			
Media	Instalación de suministro	En caso de falla en el suministro de electricidad prolongado, no hay opción alternativa para continuar con los servicios de la DCB	Medio	AR	3 meses	Se deberán elaborar procedimientos a llevar a cabo en caso de que se de notificación de baja de energía y/o después de fallas imprevistas. Los equipos de cómputo de la DCB deberán de
		No existe documentación que indique los procedimientos a seguir en caso de aviso previo de falla en el suministro de electricidad	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		No existe documentación que indique los procedimientos a seguir cuando se recupere el suministro de electricidad después de una falla	Medio			contar con protecciones en caso de variaciones de voltaje y/o falla. Se debe incluir dentro de las políticas de seguridad
		No todos los equipos de la DCB cuentan con sistemas de regulación de voltaje y/o prevención en cortes de energía	Medio			
Media	Gestión de capacidades	Ciertos servidores cuentan con versiones de SO obsoletas	Bajo	AR	Indefinido	Se deberá de contar con las últimas versiones y actualizaciones del software utilizado en la DCB
		Ciertos equipos tienen como sistema operativo versiones de MS Windows (Windows 95 / 98 / Me)que ya no son mantenidas por Microsoft, por lo que ya no son publicados parches de seguridad para éstas.	Bajo			
		Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Bajo			
		Es posible la lectura de las bitácoras de eventos en equipos con Windows 2000	Bajo			
		Es posible la enumeración de los servicios que se encuentran activos en equipos Wndows 2000, a través de sesiones nulas	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos del Sistema	Bajo			
		Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario	Bajo			
		Ciertos equipos tienen instalada una versión de MathCad (12, 13 y 13.1) que es vulnerable a cambios de contraseñas en archivos protegidos, remoción completa de protecciones y acceso a información.	Bajo			
		En la gran mayoría de equipos se tienen instaladas versiones de MS Office que no son actualizadas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Medio			
		En ciertos equipos se tienen instaladas versiones de Open Office que son obsoletas, por lo que son propensas a la explotación de una serie de vulnerabilidades conocidas	Bajo			
		En ciertos equipos se tiene instalado Autocad (2005 y 2006) que cuenta con una vulnerabilidad no divulgada que permite a un atacante obtener privilegios elevados	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		La mayoría de los equipos tienen instaladas versiones obsoletas de Adobe Acrobat que cuentan con una serie de vulnerabilidades conocidas	Medio			
		La gran mayoría de los equipos cuentan con una versión de Kaspersky Antivirus (2008), que cuenta con una vulnerabilidad que permite a un usuario local, obtener privilegios del sistema	Bajo			
		En ciertos equipos se encuentra instalado Avira Antivir, que cuenta con una vulnerabilidad que permite la elevación de privilegios.	Bajo			
		Ciertos equipos cuentan McAfee Antivirus que cuenta con vulnerabilidades que permiten a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos cuentan con Norton Antivirus, que cuenta con vulnerabilidades permiten a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos tienen instalados versiones de MySQL con vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		En ciertos equipos se tienen instaladas versiones de MSN Live Messenger, que son vulnerables a ataques DoS del servicio	Medio			
		En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción	Bajo			
		En ciertos equipos se tienen instalada una versión de Nero Media Player, que es vulnerable a DoS de la aplicación	Bajo			
		No se cuenta con una política escrita de requerimientos mínimos para el acceso a los servicios de la red	Medio			
Media	Controles de red	Ciertos equipos escuchan en el puerto 137 y contestan a peticiones NetBIOS nbtscan	Bajo	AR	6-9 meses	Se deberán de implantar y/o actualizar firewalls en puntos críticos de la red de la DCB.
		Obtención de información de sistema operativo de distintos equipos de la red de la DCB	Bajo			Se pueden colocar IDS´s en puntos de salida de las distintas subredes de la DCB
		Ciertos equipos cuentan con los protocolos CIFS o SMB, utilizados para compartir archivos.	Medio			Se deberá de colocar un monitor de la red en tiempo real.

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Es posible el acceso a distintos equipos mediante sesiones nulas y/o cuentas de invitado	Bajo			
		Ciertos equipos responden a peticiones SMB para la obtención del host SID	Bajo			
		Es posible acceder a ciertos equipos mediante usuarios invitados, utilizando cuentas aleatorias	Bajo			
		Ciertos equipos tienen una o más carpetas compartidas de Windows. Dependiendo de los privilegios de dichas carpetas es posible la lectura/escritura remotamente	Medio			
		Ciertos equipos permiten el acceso al Registro de Windows mediante ciertas combinaciones de login / contraseña	Bajo			
		Mediante ciertas herramientas, es posible identificar archivos compartidos de Office	Bajo			
		Posibles conexiones al puerto 1031 tcp	Bajo			
		Posibles conexiones al puerto 2103 tcp	Bajo			
		Posibles conexiones al puerto 1026 tcp	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Posibles conexiones al puerto 2107 tcp	Bajo			
		Posibles conexiones al puerto 2105 tcp	Bajo			
		Posibles conexiones al puerto 135 tcp	Bajo			
		Utilización de herramientas para la identificación del tipo y versión de servidores web	Medio			
		Los métodos TRACK y TRACE están habilitados en ciertos equipos con servidores web. Son vulnerables a ataques XST (Cross Site Tracking), que pueden ser usados para la obtención sin autorización de credenciales	Medio			
		Es posible la detección de servidores VMWare en ciertos equipos mediante peticiones al puerto 912	Bajo			
		Es posible la detección de servidores web mediante peticiones a los puertos 80 y 443	Bajo			
		Ciertos equipos cuentan con certificados SSL expirados o a expirar prontamente, relacionados a servicios	Bajo			
		Ciertos equipos cuentan con protocolos de cifrado de tráfico de red como SSL anticuados (SSLv2)	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos que utilizan SSL hacen uso de protocolos que realizan cifrados débiles	Bajo			
		Ciertos equipos son vulnerables a desbordamiento de buffer, que permite ejecutar código arbitrario con los privilegios del sistema	Bajo			
		Ciertos equipos cuentan con vulnerabilidades en SMB de corrupción de memoria, que permiten la ejecución de código arbitrario o una denegación de servicio	Bajo			
		Ciertos equipos Windows contienen una falla en el servicio de Cliente de Web	Bajo			
		Ciertos equipos Windows contienen una falla en el servicio de cola de impresión	Bajo			
		Ciertos equipos Windows contienen una falla en la implementación SMB	Bajo			
		Ciertos equipos Windows contienen una versión del protocolo SMB (SMBv2), que cuenta con una serie de vulnerabilidades que permiten la ejecución de código arbitrario	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos Windows contienen una falla en la interfaz RPC que permite ejecución de código arbitrario y/o lograr privilegios del Sistema	Bajo			
		Ciertos equipos cuentan con servidores web que hacen uso de versiones de PHP obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Medio			
		Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Medio			
		Ciertos equipos hacen uso de la distribución Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de desbordamiento de buffer	Bajo			
		Es posible la detección de equipos con servicios SMTP activos	Bajo			
		Ciertos equipos que manejan el protocolo SNMP cuentan con los nombres de comunidades por default (private y public)	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos son vulnerables a ataques de Etherleak (cuando una NIC rellena las tramas con información de paquetes anteriores o con información de la memoria del kernel, en lugar de con bytes nulos)	Bajo			
		Ciertos equipos reportan las versiones de los servidores web utilizados mediante páginas de error	Medio			
		Ciertos equipos cuentan con servidores web que hacen uso de versiones de Apache Tomcat obsoletas y que cuentan con una serie de vulnerabilidades conocidas	Bajo			
		Es posible la obtención de información de servidores web mediante peticiones al puerto 5353 udp	Bajo			
		Es posible la obtención de información de servidores DNS	Bajo			
		Un servidor DNS responde a cualquier petición	Bajo			
		Posible identificación de cuentas y servicios mediante el servicio ident (auth)	Bajo			
		Es posible la obtención de información de servidores SSH	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos que cuentan con el servicio SSH habilitado son vulnerables a ataques de secuestro de sesiones X11	Bajo			
		En ciertos equipos Windows que cuentan con un servidor de protocolo de escritorio remoto, son vulnerables a ataques de hombre en medio	Bajo			
		Ciertos equipos Wndows cuentan con el servicio de terminales remotas, que es propenso a ataques de hombre en medio	Bajo			
		Ciertos equipos con el servicio SSH, cuentan con una versión insegura del protocolo (SSHv1)	Bajo			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que es vulnerable a desbordamientos de buffer remotos cuando recibe un paquete malicioso SMB	Bajo			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que permite a un atacante el acceso a archivos arbitrarios fuera de las rutas compartidas permitidas	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que, al momento de recibir una petición FindNextPrintChangeNotify() sin haber recibido previamente una llamada FindFirstPrintChangeNoticy() puede ocasionar un DoS	Bajo			
		Ciertos equipos con el servicio FTP habilitado, permiten que las credenciales de los usuarios sean transmitidas en claro	Bajo			
		En ciertos equipos es posible montar volúmenes NFS sin contar con privilegios de root	Bajo			
		En ciertos equipos con el protocolo FTP habilitado, se permiten accesos anónimos	Medio			
		Algunos servidores web son vulnerables a ataques de directorio transversal	Medio			
		En ciertos equipos es posible listar el software instalado mediante SNMP	Bajo			
		Ciertos equipos tienen instalado Common Management Agent, un componente del manejador de seguridad del sistema de McAfee. Éste contienen una serie de vulnerabilidades que pueden permitir a un atacante causar un DoS,	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		lanzar un ataque de directorio transversal y/o ejecutar código arbitrario				
		Ciertos equipos Windows cuentan con versiones del Task Scheduler vulnerables a la ejecución de código arbitrario	Bajo			
		Ciertos equipos tienen habilitada la opción de SMTP relay	Bajo			
		Es posible la identificación de versiones de los servidores SQL en Windows	Bajo			
		Ciertos equipos responden a peticiones WMI (Windows Management Instrumentation)	Bajo			
		Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos Windows, cuentan con versiones del servicio Plug and Play que permite la ejecución de código arbitrario y elevación de privilegios	Bajo			
		Es posible la lectura de las bitácoras de eventos en equipos con Windows 2000	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Es posible la enumeración de los servicios que se encuentran activos en equipos Wndows 2000, a través de sesiones nulas	Bajo			
		Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos del Sistema	Bajo			
		Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario	Bajo			
		Existen equipos con servidores web vulnerables a ataques de directorio transversal	Medio			
		Ciertos equipos tienen habilitado el servicio de telnet	Medio			
		La mayoría de los equipos tienen instaladas versiones obsoletas de Adobe Acrobat que cuentan con una serie de vulnerabilidades conocidas	Medio			
		La gran mayoría de los equipos cuentan con una versión de Kaspersky Antivirus (2008), que cuenta con una vulnerabilidad que permite a un usuario local, obtener privilegios del sistema	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos cuentan McAfee Antivirus que cuenta con vulnerabilidades que permiten a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos cuentan con Norton Antivirus, que cuenta con vulnerabilidades permiten a la ejecución de código arbitrario y/o DoS	Bajo			
		En ciertos equipos se tienen instaladas versiones de MySQL que cuentan con una serie de vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado	Bajo			
		En ciertos equipos se tienen instaladas versiones de MSN Live Messenger, que son vulnerables a ataques DoS del servicio	Medio			
		En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción de datos	Bajo			
		En ciertos equipos se tienen instalada una versión de Nero Media Player, que es vulnerable a DoS de la aplicación	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos cuentan con versiones de Samba (2.2.7) que son vulnerables a ataques de directorio transversal que permiten acceder a directorios protegidos, DoS, ejecución de código arbitrario.	Bajo			
		Ciertos equipos cuentan con versiones de Samba (3.0.3) que son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios	Bajo			
		Ciertos equipos cuentan con una versión de Apache Tomcat (5.5.26) que es vulnerable a ataques XSS	Bajo			
		Ciertos equipos cuentan con una versión de Subversion (1.5.1) que es vulnerable a ejecución de código arbitrario	Bajo			
		Ciertos equipos cuentan con una versión del proxy Squid (2.5) que es vulnerable a ataques Dos, suplantación de IP, accesos no autorizados y divulgación de información no autorizada	Medio			
		Existen equipos con información valiosa para la DCB que cuentan con IPs reales, por lo que podrían ser accedidos desde fuera de la red de la División	Alto			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		No se realiza un monitoreo adecuado del tráfico en la red de la DCB	Medio			
		No hay control alguno para evitar la suplantación de IPs reales asignadas a la DCB	Medio			
Media	Gestión de medios removibles	No se cuentan con políticas escritas de respaldos de información, protección y verificación de éstos	Medio	AR	3 meses	En el caso de baja o cambio de equipo que maneje información valiosa para la DCB, el disco duro deberá de ser destruido o formateado mínimo diez veces, para que así no pueda ser recuperada la información y sea divulgada a usuarios no autorizados Además se requiere la elaboración de procedimientos de gestión de los medios removibles y su información contenida, commo discos duros, CD´s, DVD´s, etc. Se debe incluir dentro de las políticas de seguridad.
		No se cuentan con políticas escritas de protección a medios de almacenamiento	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
Media	Procedimientos de manipulación de la información	No se cuentan con políticas escritas de respaldos de información, protección y verificación de éstos	Medio	AR y CC	3 meses	Deberán de elaborarse procedimientos para la correcta manipulación de la información de la DCB. Se debe incluir dentro de las políticas de seguridad.
		No se cuentan con políticas escritas de protección a medios de almacenamiento	Medio			
Media	Supervisión del uso del sistema	Cualquier usuario puede instalar aplicaciones en los equipos a los que tienen acceso	Medio	AR	3 meses	Se deberán de implantar candados en los sistemas operativos y/o aplicaciones que puedan contener información valiosa para la DCB
		No se cuenta con control alguno respecto a las aplicaciones que pueden ser instaladas o no en los equipos de la DCB dentro de las áreas de coordinaciones, secciones académicas, laboratorios y cubículos en general.	Medio			
Media	Controles contra el código malicioso	No se cuenta con control alguno respecto a las aplicaciones que pueden ser instaladas o no en los equipos de la DCB dentro de las áreas de coordinaciones, secciones académicas, laboratorios y cubículos en general.	Medio	AR	3 meses	Se deberán de implantar candados en los sistemas operativos y/o aplicaciones que puedan contener información valiosa para la DCB.

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Los profesores y alumnos comparten información por medio de dispositivos de almacenamiento como memorias flash, por los cuales se realiza la propagación de virus, spyware, caballos de troya, etc...	Medio			Se debe incluir en las políticas de seguridad
Media	Autenticación de usuarios para conexiones externas	Es posible el acceso a distintos equipos mediante sesiones nulas y/o cuentas de invitado	Bajo		6 meses	Se deberá de implantar un control de acceso adecuado, de acuerdo a la aplicación y dependiendo del grado de nivel crítico y/o sensitividad de éstas
		Es posible acceder a ciertos equipos mediante usuarios invitados, utilizando cuentas aleatorias	Bajo			
		Ciertos equipos permiten el acceso al Registro de Windows mediante ciertas combinaciones de login / contraseña	Bajo			
		Los métodos TRACK y TRACE están habilitados en ciertos equipos con servidores web. Son vulnerables a ataques XST (Cross Site Tracking), que pueden ser usados para la obtención sin autorización de credenciales	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos Windows contienen una falla en el servicio de Cliente de Web	Bajo			
		Ciertos equipos Windows contienen una falla en el servicio de cola de impresión	Bajo			
		Ciertos equipos Windows contienen una falla en la implementación SMB	Bajo			
		Ciertos equipos Windows contienen una versión del protocolo SMB (SMBv2), que cuenta con una serie de vulnerabilidades que permiten la ejecución de código arbitrario	Bajo			
		Ciertos equipos Windows contienen una falla en la intefaz RPC que permite ejecución de código arbitrario y/o lograr privilegios del Sistema	Medio			
		Ciertos equipos hacen uso de la distribución Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de desbordamiento de buffer	Bajo			
		Ciertos equipos reportan las versiones de los servidores web utilizados mediante páginas de error	Medio			
		Un servidor DNS responde a cualquier petición	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		En ciertos equipos Windows que cuentan con un servidor de protocolo de escritorio remoto, son vulnerables a ataques de hombre en medio	Bajo			
		os equipos Wndows cuentan con el servicio de terminales remotas, que es propenso a ataques de hombre en medio	Bajo			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que es vulnerable a desbordamientos de buffer remotos cuando recibe un paquete malicioso SMB	Bajo			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que permite a un atacante el acceso a archivos arbitrarios fuera de las rutas compartidas permitidas	Medio			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que, al momento de recibir una petición FindNextPrintChangeNotify() sin haber recibido previamente una llamada FindFirstPrintChangeNoticy() puede ocasionar un DoS	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Algunos servidores web son vulnerables a ataques de directorio transversal	Medio			
		Ciertos equipos tienen instalado Common Management Agent, un componente del manejador de seguridad del sistema de McAfee. Éste contienen una serie de vulnerabilidades que pueden permitir a un atacante causar un DoS, lanzar un ataque de directorio transversal y/o ejecutar código arbitrario	Bajo			
		Ciertos equipos Windows cuentan con versiones del Task Scheduler vulnerables a la ejecución de código arbitrario	Bajo			
		Ciertos equipos responden a peticiones WMI (Windows Management Instrumentation)	Bajo			
		Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos del Sistema	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario	Bajo			
		Existen equipos con servidores web vulnerables a ataques de directorio transversal	Medio			
		Ciertos equipos cuentan McAfee Antivirus que cuenta con vulnerabilidades que permiten a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos cuentan con Norton Antivirus, que cuenta con vulnerabilidades permiten a la ejecución de código arbitrario y/o DoS	Bajo			
		En ciertos equipos se tienen instaladas versiones de MySQL que cuentan con una serie de vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado	Bajo			
		En ciertos equipos se tienen instaladas versiones de MSN Live Messenger, que son vulnerables a ataques DoS del servicio	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción de datos	Bajo			
		En ciertos equipos se tienen instalada una versión de Nero Media Player, que es vulnerable a DoS de la aplicación	Bajo			
		Ciertos equipos cuentan con versiones de Samba (2.2.7) que son vulnerables a ataques de directorio transversal que permiten acceder a directorios protegidos, DoS, ejecución de código arbitrario.	Bajo			
		Ciertos equipos cuentan con versiones de Samba (3.0.3) que son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios	Bajo			
		Ciertos equipos cuentan con una versión de Apache Tomcat (5.5.26) que es vulnerable a ataques XSS	Bajo			
		Ciertos equipos cuentan con una versión de Subversion (1.5.1) que es vulnerable a ejecución de código arbitrario	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos cuentan con una versión del proxy Squid (2.5) que es vulnerable a ataques Dos, suplantación de IP, accesos no autorizados y divulgación de información no autorizada	Medio			
Media	Uso de los recursos del sistema	Ciertos equipos son vulnerables a desbordamiento de buffer, que permite ejecutar código arbitrario con los privilegios del sistema	Bajo	AR	3 meses	Se deberá de cambiar el equipo obsoleto, que debido a sus capacidades, no pueda utlizar un sistema operativo reciente. Se debe incluir dentro de las políticas de seguridad.
		Ciertos equipos Windows contienen una falla en el servicio de Cliente de Web	Bajo			
		Ciertos equipos Windows contienen una falla en el servicio de cola de impresión	Bajo			
		Ciertos equipos Windows contienen una falla en la implementación SMB	Bajo			
		Ciertos equipos Windows contienen una versión del protocolo SMB (SMBv2), que cuenta con una serie de vulnerabilidades que permiten la ejecución de código arbitrario	Bajo			
		Ciertos equipos Windows contienen una falla en la intefaz RPC que permite ejecución de código arbitrario y/o lograr privilegios del Sistema	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Ciertos equipos hacen uso de la distribución Apache XAMPP, que bajo ciertas condiciones es vulnerable a ataques de desbordamiento de buffer	Bajo			
		En ciertos equipos Windows que cuentan con un servidor de protocolo de escritorio remoto, son vulnerables a ataques de hombre en medio	Bajo			
		Ciertos equipos Wndows cuentan con el servicio de terminales remotas, que es propenso a ataques de hombre en medio	Bajo			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que es vulnerable a desbordamientos de buffer remotos cuando recibe un paquete malicioso SMB	Bajo			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que permite a un atacante el acceso a archivos arbitrarios fuera de las rutas compartidas permitidas	Medio			
		Ciertos equipos con el servicio Samba habilitado, cuentan con una versión obsoleta que, al momento de recibir una petición FindNextPrintChangeNotify()	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		sin haber recibido previamente una llamada FindFirstPrintChangeNoticy() puede ocasionar un DoS				
		En ciertos equipos es posible montar volúmenes NFS sin contar con privilegios de root	Bajo			
		Algunos servidores web son vulnerables a ataques de directorio transversal	Medio			
		Ciertos equipos tienen instalado Common Management Agent, un componente del manejador de seguridad del sistema de McAfee. Éste contienen una serie de vulnerabilidades que pueden permitir a un atacante causar un DoS, lanzar un ataque de directorio transversal y/o ejecutar código arbitrario	Bajo			
		Ciertos equipos Windows cuentan con versiones del Task Scheduler vulnerables a la ejecución de código arbitrario	Bajo			
		Ciertos equipos tienen habilitada la opción de SMTP relay	Bajo			
		Ciertos equipos responden a peticiones WMI (Windows Management Instrumentation)	Bajo			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		Existen equipos con Windows 2000 y MSN Messenger que son vulnerables a la ejecución de código arbitrario y/o DoS	Bajo			
		Ciertos equipos Windows, cuentan con versiones del servicio Plug and Play que permite la ejecución de código arbitrario y elevación de privilegios	Bajo			
		Es posible la lectura de las bitácoras de eventos en equipos con Windows 2000	Bajo			
		Es posible la enumeración de los servicios que se encuentran activos en equipos Wndows 2000, a través de sesiones nulas	Bajo			
		Ciertos equipos con Windows 2000 contienen una falla en el servicio LSASS que permite la ejecución de código arbitrario con permisos del Sistema	Bajo			
		Ciertos equipos con Windows 2000 contienen librerías ASN.1 que permiten la ejecución de código arbitrario	Bajo			
		Existen equipos con servidores web vulnerables a ataques de directorio transversal	Medio			

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
		En ciertos equipos se encuentra instalado Avira Antivir, que cuenta con una vulnerabilidad que permite la elevación de privilegios.	Bajo			
		En ciertos equipos se tienen instaladas versiones de MySQL que cuentan con una serie de vulnerabilidades, que permiten la ejecución de código arbitrario, DoS, inserción de archivos, elevación de privilegios y acceso no autorizado	Bajo			
		En ciertos equipos se tienen instaladas versiones obsoletas de Skype, que son vulnerables a ejecución de código arbitrario y a inserción de datos	Bajo			
		Ciertos equipos cuentan con versiones de Samba (3.0.3) que son vulnerables a ataques de directorio transversal, DoS, ejecución de código arbitrario y elevación de privilegios	Bajo			
Baja	Asignación de responsabilida-des relativas a la seguridad de la información	No se cuenta con la debida asignación de responsabilidades en seguridad informática	Medio	CC	3 meses	Deberán de asignarse las debidas responsabilidades de seguridad al personal correspondiente a la DCB. Se debe incluir dentro de las políticas de seguridad.

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
Baja	Inventario de activos	No se cuenta con un correcto inventario de activos informáticos	Bajo	CC	3 meses	Se deberá de elaborar un inventario con los activos de cómputo de la DCB. .Se debe incluir dentro de las políticas de seguridad
Baja	Propiedad de activos	No se cuenta con un correcto inventario de activos	Bajo	CC	3 meses	Se deberá de elaborar un inventario con los activos de cómputo de la DCB. .Se debe incluir dentro de las políticas de seguridad
Baja	Directrices de clasificación	No se cuenta con una clasificación de los recursos informáticos, con base en su nivel crítico y/o sensibilidad	Medio	RTCA y CC	Indefinido	Sujeto a aprobación
Baja	Etiquetado y manipulación de la información	No se cuenta con una clasificación de los recursos informáticos, con base en su nivel crítico y/o sensibilidad	Medio	RTCA y CC	Indefinido	Sujeto a aprobación
Baja	Responsabilidad del cese o cambio	No se cuentan con procedimientos de terminación de empleados o cambios de éstos (baja de claves, contraseñas, devolución de activos, privilegios, etc…)	Medio	AR y CC	3 meses	Se deberán de elaborar procedimientos para el cese o cambio de personal de la DCB. Se debe incluir dentro de las políticas de seguridad.

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
Baja	Devolución de activos	No se cuentan con procedimientos de terminación de empleados o cambios de éstos (baja de claves, contraseñas, devolución de activos, privilegios, etc…)	Medio	AR y CC	3 meses	Se deberán de elaborar procedimientos para el cese o cambio de personal de la DCB. Se debe incluir dentro de las políticas de seguridad.
Baja	Retiro de los derechos de acceso	No se cuentan con procedimientos de terminación de empleados o cambios de éstos (baja de claves, contraseñas, devolución de activos, privilegios, etc…)	Medio	AR y CC	3 meses	Se deberán de elaborar procedimientos para el cese o cambio de personal de la DCB. Se debe incluir dentro de las políticas de seguridad.
Baja	Protección contra amenazas externas y de origen ambiental	No existe documentación que indique los procedimientos a seguir antes y después de que ocurra un sismo	Bajo	AR	3 meses	Se deberán elaborar procedimientos para antes y después de un sismo. Se debe incluir dentro de las políticas de seguridad
Baja	Separación de los recursos de desarrollo, prueba y operación	No se cuenta con equipo específicamente destinado a desarrollo y/o pruebas	Medio	AR	Indefinido	Se deberá otorgar el equipo suficiente para el desarrollo y/o pruebas de las aplicaciones de la DCB

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
Baja	Copias de seguridad de la información	No se cuentan con políticas escritas de respaldos de información, protección y verificación de éstos	Medio	AR	3 meses	Se deberán de realizar respaldos periodicos de información valiosa para la DCB, así como la verificación de éstos.Se debe incluir dentro de las políticas de seguridad
Baja	Políticas y procedimientos de intercambio de información	La información valiosa para la DCB no es almacenada de forma cifrada	Medio	CC y AR	3 meses	Se deberá de elaborar procedimientos de cifrado para la información valiosa de la DCB. Se debe incluir dentro de las políticas de seguridad
Baja	Registro de auditorías	En ciertos servidores y aplicaciones no se lleva un historial de incidentes de seguridad y sus resoluciones	Bajo	AR	3 meses	Se deberá elaborar un procedimiento a aplicar en caso de incidentes de seguridad dentro de la DCB. Se debe incluir dentro de las políticas de seguridad
Baja	Aceptación del sistema	No se cuenta con una política escrita de requerimientos mínimos para el acceso a los servicios de la red	Medio	AR y CC	3 meses	Se deberán establecer los requerimientos mínimos para que un equipo pueda tener acceso a los

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
						servicios de cómputo de la DCB. Se debe incluir dentro de las políticas de seguridad
Baja	Segregación de las redes	Los equipos críticos o sensibles de la DCB no se encuentran debidamente segregados	Medio	AR	Indefinido	Dependerá de los planes de expansión y/o actualización de la red de la DCB
Baja	Control de la conexión a la red	No se cuenta con un control adecuado establecido de conexión de equipos personales a la red	Medio	AR y CC	3 meses	Se deberán establecer un procedimiento para que un equipo pueda tener acceso a la red de la DCB. Se debe incluir dentro de las políticas de seguridad
Baja	Procedimientos seguros de inicio de sesión	Ciertos equipos de funcionarios de la DCB no cuentan con controles de acceso para restringir privilegios a ayudantes	Medio	AR y CC	3 meses	Se deberán de implantar candados en los sistemas operativos y/o aplicaciones que puedan contener información valiosa para la DCB
Baja	Identificación y autenticación de usuario	Ciertos equipos de funcionarios de la DCB no cuentan con controles de acceso para restringir privilegios a ayudantes	Medio	AR y CC	3 meses	Se deberán de implantar candados en los sistemas operativos y/o aplicaciones que puedan contener

Prioridad de Acción	Control	Riesgos Asociados	Nivel de Riesgo	Personal Responsable	Tiempo de Implantación Sugerido	Comentarios
						información valiosa para la DCB
Baja	Notificación de los eventos de seguridad de la información	No se cuenta con procedimientos escritos en caso de incidentes de seguridad	Medio	AR	3 meses	Se deberá de elaborar un procedimiento para una pronta notificación, evaluación, corrección y registro de los incidentes de seguridad que ocurran en la DCB.
Baja	Aprendizaje de los incidentes de seguridad de la información	En ciertos servidores y aplicaciones no se lleva un historial de incidentes de seguridad y sus resoluciones	Bajo	AR	3 meses	Se deberá de elaborar un procedimiento para una pronta notificación, evaluación, corrección y registro de los incidentes de seguridad que ocurran en la DCB.
Baja	Continuidad del negocio y evaluación de riesgos	No se cuenta con una política de realización de estudios de gestión de riesgos	Bajo	AR	3 meses	Se deberá de establecer una periodicidad de la elaboración de un estudioo de gestión de riesgos en la DCB. Se debe incluir dentro de las políticas de seguridad.

CONCLUSIONES

La implantación de este estudio de gestión de riesgos queda sujeta a aprobación de la Jefatura de la División de Ciencias Básicas.

Como producto final, se propone un programa que indica los controles seleccionados para mitigar a niveles aceptables los riesgos relacionados, así como tiempos sugeridos y responsables de dichas tareas.

Se encontraron ciertos puntos de consideración, como la urgencia de las Políticas de Seguridad y su difusión, ya que servirá como normatividad en cualquier asunto relacionado a la seguridad informática. Así como los procedimientos relacionados.

También la necesidad de colocar controles de seguridad técnicos en la red, para así poder monitorear el tráfico en ésta, y así evitar oportunamente posibles ataques que pudieran afectar gravemente la misión y las principales actividades de la División.

En general se encontró que el estado actual de la seguridad informática en la División no es malo, pero requiere de un marco sobre el cual basarse, además de la necesidad de una concientización a todo el personal de la importancia de la seguridad informática y hacerles ver que es un proceso continuo y que engloba a la totalidad de la División, un solo equipo que logre ser comprometido podría afectar gravemente a la misión de la División, que finalmente es la impartición de las asignaturas de las ciencias básicas para que los alumnos de la Facultad tengan unas bases fuertes y puedan aplicarlas alrededor de toda su carrera como universitarios.

Se observó que se requiere la elaboración de un Plan de Continuidad del Negocio (BCP) y/o un Plan de Recuperación de Desastres (DRP) en áreas donde se detectaron equipos con nivel crítico o sensibilidad a tomar en cuanta, como el Taller para la Docencia y el Taller de Cómputo para Académicos.

Representa un primer paso para la obtención de un nivel de seguridad óptimo en la DCB y servirá como base para trabajos futuros, por ejemplo un nuevo estudio de gestión de riesgos (con la clasificación de nivel crítico y sensibilidad importantes de los recursos informáticos llevada a cabo por las altas autoridades), en caso de la aprobación, la elaboración de un BCP, un DRP y para tomarse en cuenta en proyectos a futuro relacionados con el cómputo en la División.

En caso de que se apruebe la propuesta, una vez terminada la implantación, se podrán identificar los riesgos residuales.

Se recomienda la elaboración subsecuente de estudios de gestión de riesgos en caso de algún cambio importante en el esquema de red, o el uso de aplicaciones nuevas que manipulen información valiosa para la DCB, con una periodicidad de año y medio, debido a que es el tiempo promedio en que se dan dichos cambios en la División.

GLOSARIO

- **Access Point.** Dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.
- **AES**. **Advanced Encryption Standard.** Algoritmo criptográfico simétrico utilizado actualmente como estándar en los EU.
- **Algoritmo Criptográfico**. Procedimientos publicados y conocidos que toman entradas, incluyendo llaves criptográficas y producen una salida cifrada.
- **Amenaza**. Cualquier circunstancia o evento con el potencial de impactar desfavorablemente las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), recursos de la organización, o individuos a través de un sistema de información vía acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicios.
- **Análisis forense**. Técnicas informáticas que buscan localizar, identificar, recolectar, analizar y examinar datos mientras se busca preservar la integridad y manteniendo una estricta cadena de mando de la información descubierta.
- **Apache**. Servidor web de distribución libre y de código abierto.
- **ARP. Address Resolution Protocol**. Protocolo que emplea un equipo para correlacionar una dirección IP con una dirección de hardware.
- **Autenticación**. Servicio de seguridad que verifica la identidad de un usuario, proceso o dispositivo, previo a permitir el acceso a un recurso.
- **BCP. Business Continuity Plan**. Plan logístico que busca el correcto funcionamiento de una organización, después de ocurrido un incidente.
- **Bell-LaPadula**. Modelo de control de acceso que busca garantizar la integridad de la información.
- **Biba**. Modelo de control de acceso que busca garantizar la integridad de la información.
- **Bind**. Servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix.
- **Biometría**. Estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos.
- **BitTorrent**. Protocolo diseñado para el intercambio de archivos punto a punto (*peer to peer* o *P2P*).
- **Bomba Lógica**. Software residente en un equipo de cómputo que desencadena ciertas acciones en el momento en que se presentan ciertas condiciones establecidas en su código.

- **Browser**. Navegador de Internet. Aplicación que sirve para acceder a páginas web.
- **BS. British Standard**. Organismo encargado de realizar y publicar estándares en el Reino Unido.
- **Buffer**. Memoria de almacenamiento temporal de información. Suele tratarse de una memoria intermedia entre un dispositivo y otro.
- **Caballo de Troya**. Código malicioso que no puede auto replicarse, que aparenta tener un propósito, sin embargo, tiene otro propósito malicioso.
- **Cableado Estructurado**. Sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus.
- **Certificado Digital**. Documento digital mediante el cual un tercero confiable, usualmente una autoridad de certificación, garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.
- **Clark-Wilson**. Modelo de control de acceso que busca garantizar la integridad de la información.
- **Cliente-Servidor**. Arquitectura donde un programa realiza peticiones a otro que le da respuesta.
- **Código Abierto**. Denominación para aquellas aplicaciones que tienen su código fuente liberado. En general, los programas de código abierto suele ser libres.
- **Confidencialidad**. Servicio de seguridad que establece que la información sólo sea accesible desde entidades (dispositivos, procesos o usuarios) autorizadas.
- **Control de Acceso**. Servicio de seguridad que otorga permisos o su revocación, para lograr acceder a un recurso.
- **Cookies**. Archivos de texto que son descargados automáticamente al navegar en una página web específica, donde se almacena cierta información sobre el visitante que la página considera importante recordar.
- **Cracker**. Persona que maliciosamente irrumpe en un sistema para lucro personal.
- **Criptoanálisis**. Estudio de los métodos para poder obtener la información en claro, a partir de información cifrada, sin conocer la información secreta con la que ésta fue cifrada.
- **Criptografía**. Ciencia de usar matemáticas para cifrar y descifrar datos.
- **Criptosistema**. Conjunto de funciones de cifrado y descifrado, llave(s), mensaje en claro y mensaje cifrado.

- **Cross Site Scripting**. Ataque donde se explota una vulnerabilidad de aplicaciones web que ocurre cuando una página despliega entradas de usuarios, que no son propiamente validadas.
- **CSI.** Computer Security Institute.
- **DES**. **Data Encryption Standard.** Algoritmo criptográfico simétrico, denominado como estándar para cifrado en 1977. Actualmente no es seguro debido a que ha sido roto mediante criptoanálisis diferencial y criptoanálisis lineal.
- **Dirección Broadcast**. Dirección IP perteneciente a una subred, cuyo tráfico dirigido a ésta es transmitido a todas las direcciones de dicha subred.
- **Dirección MAC**. Identificador de 48 bits (6 bytes) que corresponde de forma única a un dispositivo de red.
- **Discrecionary Access Control (DAC)**. Tipo de control de acceso, donde el dueño del recurso puede otorgar a otros individuos o procesos, permisos sobre éste.
- **Disponibilidad**. Servicio de seguridad que indica que la información puede ser accesible y utilizable por entidades autorizadas, en el momento que sea requerida.
- **DHCP. Dynamic Host Configuration Protocol**. Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente
- **DNS. Domain Name System**. Conjunto de protocolos y servicios para la identificación/conversión de una dirección de internet expresada en lenguaje natural por una dirección IP.
- **DoS. Denial of Service**. Negación de servicio, es decir, la prevención del acceso autorizado a recursos o la demora de procesos que requieren rapidez en su operación.
- **DRP. Disaster Recovery Plan**. Plan que busca la restitución de las capacidades normales de una organización en el menor tiempo posible, después de ocurrido un desastre.
- **El Gamal**. Algoritmo criptográfico asimétrico cuya aplicación principal es la de firma digital.
- **Equipo Activo**. Dispositivos de red.
- **Exploit**. Pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico.
- **Falso positivo**. Una alerta que incorrectamente indica que está ocurriendo actividad maliciosa.
- **Firewall**. Dispositivo o sistema que manipula el flujo de tráfico entre redes.

- **Firma Digital**. Datos adjuntados, o transformación criptográfica utilizada para asegurar la autenticidad de origen, integridad y no repudio de un documento.
- **Firmware**. Programa que es grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.
- **Fragmentación IP**. Distribución de un paquete IP entre varios bloques de datos, si su tamaño sobrepasa la **unidad máxima de transferencia** (Maximum Transfer Unit - MTU) del canal.
- **FTP. File Transfer Protocol**. Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.
- **Función Hash**. Función que mapea una cadena de bits de longitud arbitraria hacia otra cadena de longitud fija. Debe de ser de un solo sentido, es decir, no tener función inversa; además de ser resistente a colisiones, es decir, que no sea computacionalmente posible que de dos cadenas distintas se obtenga como resultado la misma cadena de salida.
- **Gusano**. Código malicioso auto-replicable, auto-propagable y auto-contenido que utiliza mecanismos de red para su propagación.
- **Hacker**. Persona apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet (*"Black hats"*). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas (*"White hats"*) y a los de moral ambigua como son los *"Grey hats"*.
- **Hash**. Véase Función Hash
- **Hash LANMAN**. Formato utilizado por Microsoft en versiones de Windows previas a Vista, utilizados para almacenar contraseñas de longitud de hasta 14 caracteres. Si la contraseña es menor a 14 caracteres, es concatenada con ceros, hasta cubrir los 14 caracteres. Dicha contraseña es dividida en 2 partes de 7 caracteres y se utiliza un algoritmo similar al DES para crear el hash.
- **Hash NT**. Formato utilizado por Windows para crear el hash de las contraseñas, primero las convierte a Unicode y utiliza el algoritmo MD4 para obtener así una cadena de 16 bytes.
- **Hombre en Medio. Man In The Middle**. Tipo de ataque en los protocolos de autenticación, donde el atacante se posiciona entre el ente que inicia la comunicación y la que responde, de manera que puede interceptar y/o alterar la información que viaja entre éstos.
- **Honeypot**. Un host que es designado para la recolección de datos sobre actividad sospechosa y no tiene usuarios autorizados aparte de los administradores de éste.

- **Host**. Equipo conectado a una red. Tiene un nombre que lo identifica, el hostname.
- **Host SID**. **Host Security Identifier**. Identificador utilizado para listar los usuarios de un dominio o listar los usuarios locales.
- **Hub**. Equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás. Son obsoletos debido a la gran cantidad de colisiones y tráfico de red que producen.
- **ICMP. Internet Control Message Protocol**. Protocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP), utilizado para enviar mensajes de errores cuando un servicio no está disponible o cuando un host no puede ser encontrado, etc.
- **IDEA**. **International Data Encryption Algorithm.** Algoritmo de cifrado por bloques.
- **IDS**. Software monitor, que busca actividades sospechosas y alerta a los administradores de éstas.
- **IEC. International Electrotechnical Commission**. Organización que prepara y publica estándares internacionales para tecnologías eléctricas, electrónicas y relacionadas.
- **IGMP**. **Internet Group Management Protocol**. Protocolo de red utilizado para intercambiar información sobre el estado de pertenencia entre enrutadores IP que admiten multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.
- **Ingeniería Social**. Consiste en persuadir o manipular a una persona para obtener datos útiles sobre ellos mismos o las empresas en donde trabajan.
- **Integridad**. Servicio de seguridad que establece que la información no ha sido alterada o destruida de manera no autorizada.
- **Impacto**. Magnitud del daño que puede ser causado por el aprovechamiento de una vulnerabilidad por una amenaza
- **Incidente de Seguridad**. Cualquier evento en el que individuos no autorizados acceden o intentan acceder a sistemas de cómputo o a recursos, los cuales no cuenta con privilegio alguno.
- **Información Crítica**. Información que requiere alta disponibilidad.
- **Información Sensible**. Información que requiere alta confidencialidad y/o integridad.
- **IPS**. Software que puede detectar actividad intrusiva, además de realizar intentos de detenerla, idealmente antes de que llegue a su objetivo.

- **IRC**. **Internet Relay Chat**. Protocolo de comunicación en tiempo real basado en texto, que permite conversar con personas en forma de texto dentro de canales IRC o de forma privada.
- **ISO**. **International Organization for Standars**. Organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.
- **Kernel**. Parte esencial de un sistema operativo que provee los servicios más básicos del sistema.
- **Latencia**. Tiempo o lapso necesario para que un paquete de información se transfiera de un lugar a otro.
- **LAN. Local Area Network**. Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar.
- **Link Aggregation**. Término usado en las redes de cómputo, que describe el uso de múltiples cales/puertos de red en paralelo, para así incrementar la velocidad más allá de los límites de un solo cable o puerto, y para incrementar la redundancia para una mayor disponibilidad.
- **LIU.** Unidad de Interconexión de Luz.
- **Máquina zombie**. Host comprometido que puede ser utilizado para lanzar ataques por terceros.
- **MD5**. Algoritmo de función hash, que produce una salida de 128 bits.
- **Middleware**. Software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas.
- **Modelo OSI**. Modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconection), proporciona a los fabricantes estándares que aseguran mayor compatibilidad e interoperatibilidad entre distintas tecnologías de red producidas a mundialmente. Consta de 7 capas: física, enlace, red, transporte, sesión, presentación y aplicación.
- **NAT. Network Address Translation**. Estándar para la utilización de una o más direcciones IP para conectar varias computadoras a una red. Cada computadora tiene una dirección IP distinta (generalmente no válida para Internet).
- **No-break.** Dispositivo que consiste en un conjunto de baterías recargables y circuitos electrónicos de inversión, que detectan el momento en que se presenta una falla en el

suministro de energía; al detectar la falla proporciona una tensión útil proveniente de la carga eléctrica almacenada en las baterías.

- **No repudio**. Servicio de seguridad que establece que las entidades involucradas en una comunicación no puedan negar su participación.
- **Oficial de Seguridad.** Persona encargada de la gestión de la seguridad informática en una organización.
- **Parche de Seguridad**. Programa que se encarga de modificar una aplicación o sistema operativo para corregirla o alterarla por algún motivo.
- **Pentest**. Véase Prueba de Penetración.
- **Phishing**. Técnicas que buscan manipular individuos para que revelen información personal mediante medios basados en cómputo.
- **PKI. Public Key Infrastructure**. Conjunto de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.
- **Prueba de Penetración**. Pruebas de seguridad, donde se intentan eludir los controles de seguridad de un sistema.
- **P2P**. Red descentralizada que no tiene clientes ni servidores fijos, sino que tiene una serie de nodos que se comportan simultáneamente como clientes y servidores de los demás nodos de la red. Cada nodo puede iniciar, detener o completar una transacción compatible.
- **RBAC**. **Role-Based Access Control.** Modelo de control de acceso basado en roles.
- **Red de Datos**. Interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.
- **RFC. Request For Comments**. Serie de documentos, donde cada uno de ellos es una propuesta oficial para un protocolo de Internet, explicándose a detalle para que, en caso de ser aceptado, éste pueda ser interpretado sin ambigüedades.
- **Riesgo**. Medida de la probabilidad de que una amenaza, a través de una vulnerabilidad, afecte el correcto funcionamiento de un sistema; y el impacto resultante de dicho evento en una organización.
- **Riesgo Residual**. Los riesgos remanentes después de que se han aplicado controles de seguridad.
- **RIPEMD**. Algoritmo de función hash, que produce una salida de 160 bits.
- **RSA**. Algoritmo criptográfico asimétrico.

- **Ruteador o Router**. Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.
- **Script**. Conjunto de instrucciones generalmente almacenadas en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución, se distinguen de los programas, pues deben ser convertidos a un archivo binario ejecutable para correrlos.
- **Service Pack (SP)**. Conjunto de actualizaciones, reparaciones y ampliaciones para una aplicación o sistema operativo específico, contenido en un solo paquete ejecutable.
- **SGSI**. **Sistema de Gestión de la seguridad de la Información.** Conjunto de políticas de administración de la información, utilizado en la serie ISO 27000.
- **SHA. Secure Hash Algoritm**. Conjunto de funciones hash relacionados con la Agencia de Seguridad Nacional de los Estados Unidos.
- **Shell**. Software que provee una interfaz para usuarios. Generalmente el término se refiere al shell del sistema operativo que provee acceso a los servicios del kernel.
- **Sniffer**. Aplicación de monitorización y de análisis para el tráfico de una red.
- **SNMP**. **Simple Network Management Protocol**. Protocolo que permite supervisar, analizar y comunicar información de estado entre una gran variedad de hosts, pudiendo detectar problemas y proporcionar mensajes de estados.
- **Spoofing**. Técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación
- **Spyware**. Código malicioso que es secretamente instalado, con el propósito de recopilar información de individuos u organizaciones sin el consentimiento del dueño.
- **Switch**. Dispositivo que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI.
- **Telnet**. Protocolo de red que sirve para acceder mediante una red a otra máquina. También es llamado así al programa cliente que utiliza el protocolo.
- **Three-way Handshake**. Procedimiento perteneciente al protocol TCP utilizado para establecer una conexión entre dos dispositivos de red.
- **TI. Tecnologías de la Información**. Conjunto de técnicas, desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos.
- **Time-Stamp**. Secuencia de caracteres, que denotan la hora y fecha en la cual ocurrió determinado evento.

- **Torrent**. Archivo utilizado por un cliente de BitTorrent u otros programas P2P que emplean el protocolo BitTorrent.
- **Traffic Padding**. Contramedida que genera datos espurios en medios de transmisión, para así hacer más difícil el análisis del tráfico y/o criptoanálisis más difícil.
- **UTP**. Par de cable de par trenzado utilizado en cableado estructurado.
- **Virus**. Código malicioso auto replicable, que se adjunta a sí mismo a un programa de aplicación u otro archivo ejecutable.
- **Vulnerabilidad**. Debilidad que puede accidentalmente desencadenada o intencionalmente explotada.
- **WMI**. **Windows Management Instrumentation.** Implementación de WBEM (Web-Based Enterprise Management) de Microsoft, una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa. Proporciona compatibilidad integrada para el Modelo de Información Común (CIM, *Common Information Model*), que describe los objetos existentes en un entorno de administración.
- **XSS.** Véase Cross Site Scripting.

REFERENCIAS

dcb.fi-c.unam.mx

www.SecurityFocus.com

www.iso27000.es

SecurityFocus.com

SecurityWatch.com

SecurityPortal.com

SANS.org

www.cert.org

icat.nist.gov

nvd.nist.gov

osvdb.org

www.kb.cert.org/vuls

insecure.org

www.caida.org

nmap.org

www.dos-attacks.com

www.databasejournal.com/features/mssql/article.php/3372131/Using-xpcmdshell.htm

www.unixwiz.net/techtips/sql-injection.html

www.mssqlcity.com/Articles/Undoc/UndocExtSP.htm

www.antiphishing.org

www.securesphere.net/download/papers/dnsspoof.htm

sectools.org/crackers.html

hackersforcharity.org/ghdb

packetstormsecurity.org

www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

standards.bz

www.csoonline.com/article/472866/Top_Network_Security_Threats_in_

www.alegsa.com.ar

Kissel, R.; "NIST IR 7298. Glossary of Key Information Security Terms"; Estados Unidos; National Institute of Standards and Technology ; 2006

Daltabuit, E.; Hernández, L.; Mallén, G; y Vázquez, J; "La Seguridad de la Información"; México; Limusa; 2007

Bishop, Matt; "Introduction to Computer Security"; Estados Unidos; Prentice-Hall; 2004

Beaver, K.; "Hacking for Dummies"; Estados Unidos; Wiley Publishing; 2004

Krutz, R,; Vines, R,; "The CISSP Prep Guide, Second Edition: Mastering the CISSP and ISSEP Exams"; Estados Unidos; Wiley Publishing; 2004

McClure, S., Scambray, J., Kurtz, G.; "Hacking Exposed: Network Security Secrets & Solutions"; Estados Unidos; McGraw-Hill; 2005

Mitnick, K.; "The Art of Deception. Controlling the Human Element of Security"; Wiley Publishing; 2002

Mitnick, K.; "The Art of Intrusion. The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers"; Wiley Publishing; 2005

Landoll, D.; "The Security Risk Assessment Handbook"; Auerbach Publications; 2006

Purdy, G.; "LINUX iptables. Pocket Reference"; O´Reilly; 2004

Schneier, B.; “Applied Cryptography: Protocols, Algorithms and Source Code in C”; Wiley Publishing; 1995

Whitaker, A.; Newman, D.; “Penetration Testing and Network Defense”; Cisco Press; 2006

Cowan, C., et al; “Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade”; Department of Science and Engineering, Oregon Graduate Institute of Science & Technology; Estados Unidos; IEEE Computer Society; 1999

Staniford, S.; Paxson, V.; Weaver, N; “How to 0wn the Internet in Your Spare Time”; Proceedings of the 11th USENIX Security Symposium; Estados Unidos; 2002

Moore, D., et al; “Inside the Slammer Worm”; IEEE Computer Society; 2003

Mirkovic, J., Martin, J., Reinher, P.; “A Taxonomy of DdoS Attacks and DdoS Defense Mechanisms”; Computer Science Department; University of California, Los Angeles, Estados Unidos; 2004

Anley, C,; “Advanced SQL Injection in SQL Server Applications”; NGSSoftware Insighyt Security Research (NISR) Publication; Estados Unidos; 2002

Anley, C.; “(more) Advanced SQL Injection”; NGSSoftware Insighyt Security Research (NISR) Publication; Estados Unidos; 2002

Dhamija, R., Tygar, J., Hearst, M.; “Why Phishing Works”; Harvard and Berkeley University; Estados Unidos, 2006

Ollmann, G,; “The Phishing Guide. Understanding & Preventing Phishing Attacks”; Next Generation Security Software Ltd.; Estados Unidos; 2004

Bowers. D., Harnett. D., Edwards. C.; “The State of Spam. A Monthly Report – January 2009”; Symantec Enterprise Security; Estados Unidos; 2009

Lueg, C.; “Spam and Antispam Measures: A Look At Potential Impacts”; University of Technology Sidney; Australia; 2003

Ollmann, G,; “The Pharming Guide. Understanding & Preventing DNS-Related Attacks by Phishers”; Next Generation Security Software Ltd.; Estados Unidos; 2005

Klein, Amit; “Cross Site Scripting Explained”; Sanctum Security Group; Estados Unidos; 2002

Kelley, P.; “ARP Poisoning”; EttercapNG; Estados Unidos; 2005

Puri, Ramneek; “Bots & Botnets: An overview”; SANS Institute Reading Room; 2003

“FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems”; Computer Security Division, Information Technology Laboratory, NIST; 2006

Alberts, C,; Dorofee, A,; Stevens, J,; Woody, C.; “Introduction to the OCTAVE Approach”; Carnegie Mellon Software Engineering Institute; Estados Unidos; 2003

“MAGERIT Versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 1 - Método”; Ministerio0d e Administraciones Públicas; Madrid, España; 2006

Devar, H.; “An Introduction to Intrusion Detection Systems”; IBM Research, Zurich Research Laboratory; Zurich, Suiza

Kohel, D.; “Cryptography”; 2008

“An Introduction to Cryptography”; Network Associates; Estados Unidos; 2000

Diffie, W., Hellman, M,; “New Directions in Cryptography”; IEEE Transactions on Information; Estados Unidos; 1976

Richardson, R.; “CSI Computer Crime & Security Survey”; Computer Security Institute; 2008

“Top Information Security Risks for 2008”; CISSP Forum & ISO27k Implementers Forum; Diciembre 2007

Baker, W.; Hylender, C.; Valentine, J.; “2008 Data Breach Investigations Report”; Verizon Business RISK Team

“The Web Hacking Incidents Database 2008”; Breach Security Inc.; 2009

“NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook”

Swanson, M,; Hash, J.; Bowen, P.; “NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems”; 2006

Swanson; “NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems”; 2001

Stoneburner, G.; Goguen, A.; Feringa, A.; “NIST SP 800-30, Risk Management Guide for Information Technology Systems”; 2002

Wack, J.; Cutler, K.; Pole, J.; “NIST SP 800-41, Guidelines on Firewalls and Firewall Policy”; 2002

Grance, T.; Kent, K.; Kim, B.; “NIST SP 800-61, Computer Security Incident Handling Guide”; 2004