Planteamiento de la Seguridad Informática

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

PLANTEAMIENTO DE LA SEGURIDAD INFORMÁTICA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

PRESENTA:

OSCAR PÉREZ LÓPEZ

DIRECTOR DE TESIS: ING. ORLANDO ZALDÍVAR ZAMORATEGUI

MÉXICO, D.F. **2008**

AGRADECIMIENTOS

Esta tesis esta dedicada a Martha y a One, mis padres, a quienes agradezco de todo corazón su apoyo, amor, cariño y comprensión. En todo momento los llevo conmigo.

Agradezco a mis hermanos Carlos y Olga por la compañía y el apoyo que me brindan. Se que cuento con ellos para siempre.

Agradezco a Dios por llenar mi vida de dicha y bendiciones.

A Irene por la chispa que enciende el fuego y la leña que ayuda a mantenerlo, por la llave que abre puertas, por la mano que acompaña y tranquiliza, por haber encontrado el amor y compartir mi existencia con ella.

Agradezco a los amigos por su confianza y lealtad.

Agradezco a la máxima casa de estudios de México, la Universidad Nacional Autónoma de México, por haberme abrigado en sus brazos de la enseñanza en la Facultad de Ingeniería, por haber hecho que sus profesores influyeran en mi formación profesional, buscando el bienestar el país con valores de profesionalismo.

Agradezco a mis maestros por su disposición y ayuda brindada.

Índice

CAPÍTULO I
INTRODUCCIÓN

1.1 HISTORIA

Se puede decir que a finales de 1980 se inició el auge en el consumo de la informática (hasta la década de los ochenta no era fácil adquirir una computadora y un módem) uniendo factores menos técnicos y se iba produciendo un aumento espectacular de gente que tenía acceso a algún tipo de sistema y con ello, un número de hackers[1] (analizan indebidamente la actividad en computadoras, programas, sistemas o redes) informáticos se fueron desarrollando. En el mismo año, 1980, miles de computadoras conectadas a la red se vieron inutilizadas durante días y las pérdidas se estimaron en millones de dólares por un problema de seguridad.

Después del incidente en 1980 y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos, la agencia DARPA (Defense Advanced Research Projects Agency) creó el CERT (Computer Emergency Response Team)[2] en 1996, un grupo formado en su mayor parte por voluntarios informáticos calificados, cuyo objetivo fue facilitar una respuesta rápida a los problemas de seguridad que afecten a hosts de Internet. Cada día se hace patente la preocupación por los temas relativos a la seguridad en la red, de los equipos y de su información.

Es por lo anterior que el tema de la seguridad en sistemas operativos y redes ha sido un factor a ser tomado en cuenta por cualquier responsable o administrador de sistemas informáticos, así como su consideración dentro de las organizaciones.

Actualmente, en la economía digital el éxito depende de la habilidad para transformarse en una organización de comercio electrónico. Cadenas de suministro en línea enlazan oficinas, empleados, clientes, socios y proveedores a través de modelos de negocios innovadores y en rápida evolución. Este cambio masivo hacia el comercio electrónico demanda una mayor protección para los activos vitales de información de las organizaciones y los sistemas que los administran. Es indispensable la disponibilidad, integridad y confidencialidad de la

[1] Tulloch Mitch. Microsoft Encyclopedia of Security. Microsoft Press, 2003

2 Tulloch Mitch, Microsoft Encyclopedia of Security, Microsoft Press, 2003

información de sistemas de la empresa, de lo contrario los clientes buscarán alguien más que les brinde estos servicios.

Los riesgos de seguridad de la información, por lo tanto, necesitan ser administrados y controlados de tal forma que se extienda la responsabilidad a través de toda la organización. Es necesario instrumentar soluciones de seguridad que se adapten y respondan rápida y fácilmente a las necesidades cambiantes nuestras y de la empresa.

Un número de empresas confrontan el reto de contar con soluciones de seguridad para sus activos de negocios en línea. Los sistemas de información son la columna vertebral universal para la economía actual conectada en red. Y aún así, son muy pocas las organizaciones que cuentan con un sistema adecuado para proteger su propiedad electrónica contra los crecientes y cada vez más sofisticados ataques y usos maliciosos.

Distintas asociaciones y grupos de seguridad han analizado el mercado para software que permite la detección de intrusos, uno de ellos es el Yankee Group que ha estimado que el mercado para software en detección de intrusos y evaluación de la seguridad ha crecido en más de $1.3 miles de millones de dólares en 2005[3].

3 Yankee Group, 2005

Antecedentes

La mayor preocupación de los administradores de sitios web de red, es el tráfico de datos[4], pero normalmente se olvidan de los mecanismos de seguridad en los browser, Outlook, Office, etc. Dada la cantidad de gente que ahora accede a los sistemas hace más latente la necesidad de medidas de control. Los índices de acceso a sitios web y sus pérdidas por incidentes se han incrementado, como se muestra en la Figura 1.1.

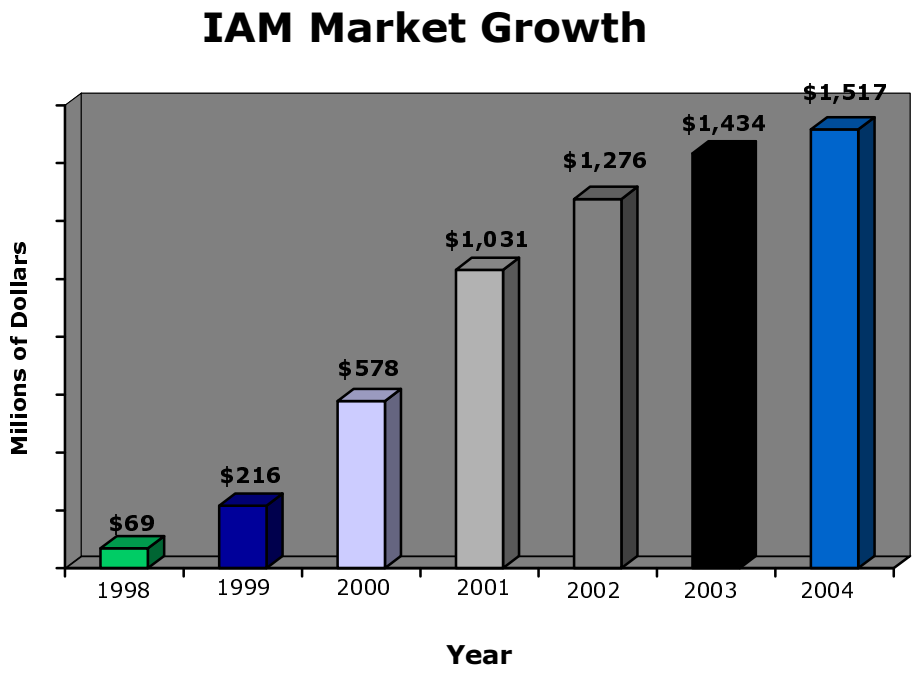


Figura 1.1 Pérdidas por problemas de seguridad
Fuente: Frost & Sullivan Research y WebSense.

Los sitios de Internet son cada vez más inseguros dado que por este medio se pueden ingresar programas que ponen en peligro instalaciones e información.

La cantidad de incidentes de seguridad que se presentan desde 1998 por gente interna de las compañías es del 30%[5], según fuente del FBI, de todos los casos reportados al CERT, como se muestra en la Figura 1.1. Es por ello necesario tomar todas las medidas preventivas para contar con información segura, dada la cantidad de problemas en software y hardware que se identifican a diario.

4 Frost & Sullivan, Websence, U.S, Marzo 2005. Pág. 10.
5 Survey, Computer Crime and Security, CSI/FBI, U.S, 1998, Pág. 34-40

A continuación, se muestran estadísticas de la tendencia por problemas de seguridad identificadas, por vulnerabilidades e incidentes[6] que se realizaron en los Estados Unidos.

Vulnerabilidades reportadas

1995-1999

Año	1995	1996	1997	1998	1999
Vulnerabilidades	171	345	311	262	417

2000-2004

Año	2000	2001	2002	2003	2004
Vulnerabilidades	1,090	2,437	4,129	3,784	3,780

Total de vulnerabilidades reportadas (1995-2004): **16,726** en las empresas con distintos sistemas operativos.

Incidentes reportados

1988-1989

Año	1988	1989
Incidentes	6	132

1990-1999

Año	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidentes	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Año	2000	2001	2002	2003
Incidentes	21,756	52,658	82,094	137,529

Total de incidentes reportados (1988-2003): **319,992**

6 Carnegie Mellon University. Patent and Trademark office, Last updated January 24, U.S. 2005.

1.2 JUSTIFICACIÓN DE TEMA

Una de las principales razones por las que existe interés en este tema es la poca información sobre la forma de implantar seguridad y la falta de medidas preventivas que se tienen en las empresas de México, ya que ahora se toma como parte de las negociaciones para la reducción de costos los outsoursing (empresas que brindan personal para servicios administrados), por lo que implica tener controles internos en desarrollos y aplicación de estándares, considerando que no es fácil contar con un área de auditoría de sistemas por los altos costos, de ahí parte la necesidad de estudiar, plantear y planear la seguridad informática.

"Dado a que se han incrementado las amenazas de los hackers en México, ya que en nuestro país se ha convertido en un botín apetitoso para los piratas del ciberespacio. En el año 2005, se extrajo información confidencial de PEMEX y CAPUFE y chantajearon con provocar explosiones en pozos de petróleo y desastres en presas. Así también, uno de los bancos más importantes del país fue estafado por más de 2.5 millones de dólares en 2005"[7].

Este trabajo está enfocado, en su mayoría, a las empresas que carecen por lo general de un proceso de planteamiento de la seguridad informática, lo que las hace vulnerables a incidentes de seguridad informática, pues los riesgos son mayores conforme se tiene un crecimiento de participación en el mercado, ya que empresas que están establecidas en Estados Unidos al instalarse en México, por citar algún ejemplo y a la falta de interés por la seguridad, hace que se tenga la probabilidad de no proporcionar información segura en los sistemas, por lo que las empresas mexicanas son un foco importante para los hackers. Dado que la seguridad informática, seguridad lógica y seguridad física son de vital importancia, es imprescindible que en México se lleven a cabo los niveles de seguridad necesarios para las empresas.

Se considera claro que siempre se tienen fallas de seguridad en los sistemas o de la propia red, aspecto que no beneficia a nadie y mucho menos a la imagen de la organización.

7 El Semanario, México, 2005. Pág. 12.

Como ejemplo, se muestra en la Figura 1.2 la cantidad de pérdidas por problemas de seguridad informática. "Se han registrado pérdidas por más de 35 mil millones de dólares desde 1998 hasta lo que va de este año, y se espera que se incremente hasta siete veces más por la evolución que los virus han presentado últimamente", aseguró Massa[8].

A continuación, se muestran en la Figura 1.2 porcentajes de gastos o pérdidas que se han tenido por crímenes informáticos.[9]

Análisis de seguridad anual (base: 500)	
$ 25 millones o más	6%
$ 10 a $ 24 millones	6%
$ 5 a $ 9.9 millones	4%
$ 1 a $ 4.9 millones	14%
$ 500,000 a $ 999,999	5%
$ 250,000 a $ 499,999	7%
$ 100,000 a $ 249,999	14%
$ 50,000 a $ 99,999	7%
menor a $ 50,000	16%
se desconoce	22%

Pérdidas monetarias por crímenes electrónicos (base: 338)	
$ 10 millones o más	3%
$ 1 millón a $ 9.9 millones	5%
$ 500,000 a $ 999,999	5%
$ 100,000 a $ 499,999	11%
menos a $ 100,000	26%
se desconoce	50%

Figura 1.2. Valor monetario por crímenes electrónicos

Crímenes electrónicos por monto. A lo largo del trabajo se plantearán los puntos habituales referentes a la seguridad; de esta forma se ofrecerá una perspectiva general en distintos entornos, en las redes por ejemplo, el funcionamiento de sus mecanismos y su correcta utilización. Se hablará sobre aspectos técnicos, que afectan directamente a la seguridad informática, como puede ser el problema del personal o la legislación vigente.

Se propone ir trabajando paulatinamente para cumplir con la mínima seguridad requerida, ayudándonos a prever, responder, atender y aprender ante cualquier incidente de seguridad. Seguramente un hacker con el tiempo suficiente, pagado o simplemente muy interesado en nuestra información, no tendría muchos problemas en acceder a ella. Debido a que, no sólo los problemas de seguridad

8 IBLNEWS, Agencias (Symantec), U.S. 2002.
9 eCrime Watch Survey, CSO magazine in cooperation with the U.S., Secret Service & CERT, Coordination Center, 2004. Pág. 9-11.

provienen del exterior de la empresa, sino también internamente, nuestro objetivo será el disminuir la probabilidad y la incidencia de algún ataque.

Es por ello que resulta indispensable la generación de un proceso, el apego a normatividades e implantación de seguridad informática por medio de herramientas de mapeo, identificando cómo actuar ante un incidente o fraude. Lo anterior es casi inevitable, ya que lo evitable es que cualquier persona sea capaz de atacar con éxito un equipo, simplemente por haber visto una película, descargado un par de páginas web y ejecutando un programa que ni ha elaborado, ni tampoco entiende.

Dado el incremento de riesgos en la red, en Internet debemos evitar incidentes y ayudar a la gente a implantar seguridad en sus sistemas, así como en las empresas para evitar ataques a sus equipos de cómputo o redes completas y explotar al 100% o próximo a este porcentaje sus sistemas.

CAPÍTULO II

OBJETIVO

2.1 ALCANCE DE TRABAJO

El presente trabajo tiene como finalidad presentar una alternativa para satisfacer la creciente necesidad de brindar nuevos esquemas de seguridad para cualquier empresa mexicana que incursiona con sistemas conectados en alguna red, con una infraestructura básica que puede acceder a Internet y a distintas redes. Esta solución permitirá proponer la forma de mantener la integridad de la empresa, de su personal, de los servicios, mediante la prevención, detección y contención de riesgos de fraude, accesos no autorizados, vandalismo, robo de información y desastres naturales.

Asimismo, ofrecer una perspectiva de la seguridad-inseguridad en entornos Unix, Windows y en redes.

Definir y determinar si el problema de seguridad informática es del personal o de la legislación vigente, así como una revisión de la legislación existente en México y la forma en que se está trabajando en esquemas de certificación.

Para cumplir con los objetivos planteados, este documento describe las características y la solución técnica de un sistema de administración de seguridad informática. Éste tendrá como primer objetivo brindar accesos seguros, identificación de vulnerabilidad y esquema de trabajo en caso de un incidente de seguridad informática, así como, las acciones a seguir en caso de desastres naturales y algún riesgo de fraude. Se definirán procedimientos para conseguir un nivel de seguridad aceptable en los esquemas de sistemas conectados en cualquier red, entendiendo por ‘aceptable’ un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los equipos de la organización fracase ante un ataque informático. El esquema de atención de incidentes de seguridad permitirá la designación de actividades, monitoreos de accesos y sucesos, identificación de incidentes, determinación del incidente, evaluación, ejecución de plan de acción, determinación de acciones de mejora, responder al incidente, declaratoria de cierre del incidente, sobre todo, el brindar y restaurar las condiciones normales de operación.

Para ello, se propone una plataforma, diagrama y flujo de trabajo que nos permitirá apegarnos a normas y estándares de seguridad, pero sobre todo un esquema de trabajo en caso de incidentes, cubriendo los estándares mínimos que hoy se tienen. La fácil implantación, la adaptabilidad a distintas formas de trabajo, el contar con las características generales de cualquier esquema de seguridad, así como su accesibilidad en costo, serán requerimientos indispensables para realizar esta propuesta.

Dada la situación actual de las empresas, la austeridad en costos, resulta ser una decisión realista el brindar una solución de seguridad que considere necesario contratar a empresas que realicen el mismo análisis y estudio de acción por incidentes, ya que éstas pueden ofrecer sus servicios y cobrar por ello, de acuerdo con los esquemas de seguridad que se pretende brindar y que consideran el mismo planeamiento que se muestra en este trabajo.

CAPÍTULO III

SEGURIDAD INFORMÁTICA

3.1 DEFINICIÓN

La Seguridad informática, es un concepto cuya definición es difícil de proporcionar, debido a la gran cantidad de factores que intervienen. Sin embargo, la seguridad es el conjunto de elementos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo estén disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo, esto es, la seguridad es un proceso y no un producto.

3.2 FUNCIONES DE LA SEGURIDAD INFORMÁTICA

Se debe buscar en las organizaciones que, con apoyo de la seguridad informática se vigilen las siguientes propiedades:

Privacidad. La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la privacidad es la divulgación de información confidencial.[10]

La acepción de privacidad puede ser definida como el ámbito de la vida personal de un individuo, que debe ser reservado y mantenerse confidencial. En cualquiera de ambas acepciones, el desarrollo de la sociedad de la información y la expansión de la informática y de las telecomunicaciones plantea nuevas amenazas, que han de ser afrontadas desde diversos puntos de vista: social, cultural, legal, etc.

Integridad. La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar[11].

Disponibilidad. La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (Denial of Service o DoS) o “tirar” el servidor.

10 Wylder, John. Introduction to Strategic Information Security, Strategic Information Security, Ed. Auerbach Publications, US, 2004, Pág. 15
11 Wylder, John. Introduction to Strategic Information Security, Strategic Information Security, Ed. Auerbach Publications, US, 2004, Pág. 20

3.3 DIVISIÓN DE LAS ÁREAS DE ADMINISTRACIÓN DE LA SEGURIDAD

Es recomendable, en la medida de lo posible, dividir las tareas de administración de seguridad en tres grandes rubros:

Autenticación. Es un proceso que verifica las entradas que son factores necesarios para identificar y asegurar la autorización dada. Es un medio para verificar las identidades de los usuarios para asegurarse que están autorizados para acceder a recursos específicos de la red. Sistemas de autenticación usan cifrado para evitar que las contraseñas sean interceptadas y conocidas por terceros[12].

Esto es, verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje. Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

Autorización. Es el hecho de que las entidades tengan acceso a los recursos de cómputo, así como a las áreas de trabajo sobre las cuales se tiene dominio.

Auditoría de sistemas. La seguridad inicia al identificar las transacciones, información que concierne al usuario y a la actividad del sistema para visualizar acciones inapropiadas[13]. También se refiere a la continua vigilancia de los servicios en producción. Mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Para ejemplificar lo anterior, sólo se debe permitir acceder a información confidencial a gente que se autentique en los equipos, llevando a cabo vigilancia en logs para identificar cuando fue de forma legal o ilegal.

12 Tulloch, Mitch. Microsoft Encyclopedia of Security, Microsoft Press, US, 2003, Pág. 35
13 Tulloch , Mitch. Microsoft Encyclopedia of Security, Microsoft Press, US, 2003, Pág. 70

3.4 FACTORES QUE INTERVIENEN EN LA SEGURIDAD

La seguridad en un sistema está determinada por los siguientes factores:

El organizacional

Usuarios

- Seguridad por la restricción de acceso a usuarios.
- La existencia de reglamentos y políticas en la empresa.
- Implantación de auditoría de sistemas que vigilan el cumplimiento del punto anterior.

La alta dirección

- La inversión en sistemas y herramientas de seguridad debe considerarse como prioridad en la organización y no como un gasto.
- La capacitación debe ser un punto importante para la gente de sistemas.
- La negociación con proveedores o outsoursing en la adquisición de equipos de cómputo o de nueva tecnología.

El software

La aplicación

- Se deben contemplar mecanismos para el control de accesos integrados.
- Identificar las mejores formas de respaldo de información que se tienen.
- Evaluar la prioridad de los recursos y sistema con los que se cuenta.

El sistema operativo

- Evaluar la conveniencia del sistema operativo (UNIX, Windows, Linux, entre otros).
- Considerar los niveles de seguridad con que cuenta cada sistema operativo, SO, mencionados en el punto anterior.
- Implantar las recomendaciones del fabricante y aplicar los parches que libere éste.
- Crear y vigilar siempre bitácoras.
- Estar informado de alertas de seguridad.

Software

- Evaluar y vigilar las estadísticas de acceso y tráfico de la red.
- Implantar firewalls u otras herramientas de seguridad y monitoreo.
- En la medida de lo posible, apoyar las conexiones cifradas.

El hardware

Hardware de red

- Elegir adecuadamente el tipo de tecnología de transporte (Ethernet, FDDI, etc.).
- Proteger muy bien el cableado, las antenas y cualquier dispositivo de red.
- Proporcionar periódicamente mantenimiento a las instalaciones.

Servidores

- Mantenerlos en condiciones de humedad y temperatura adecuadas.
- Establecer políticas de acceso físico a servidores.
- Contemplar y usar los soportes de revisión contratados en la adquisición de equipos de cómputo.

Éstos son aspectos importantes a considerar para el seguimiento de puntos de control que nos permitirán administrar correctamente cada una de las actividades con consultores, administradores, outsoursing o la misma auditoría de sistemas.

3.5 VULNERABILIDAD

Cada ocasión que se tiene la posibilidad de atacar y explorar información de nuestros sistemas se habla de vulnerabilidad[14].

Los elementos vulnerables a los ataques son todos aquellos que componen un sistema informático, es decir, hardware, software, personal dedicado y datos.

A continuación, se describen algunas formas de ataque por intrusos.

Ataques al hardware. Se pueden producir de forma intencionada o no. Incendios fortuitos en los sistemas, errores físicos, rotura física de cables, etc.

14 Tulloch, Mitch. Microsoft Encyclopedia of Security, Microsoft Press 2003, US, Pág. 289

Ataques al software. Se pueden centrar en programas del sistema operativo, los cuales son de utilidad o del usuario.

A continuación, describimos algunos tipos de ataques:

Bomba lógica. El programa incluye instrucciones que al cumplirse una condición, provocan una distorsión del funcionamiento del programa, que normalmente, deriva en daños a la computadora que lo ejecuta. Esta técnica es usada por algunos programadores, introducen en la aplicación un código que se activa en una fecha determinada para que, si no ha cobrado por su trabajo ese día, destruya la información de la computadora en donde se instaló la bomba lógica.

Virus. Código malicioso que infecta archivos dentro del sistema[15]. La conectividad entre computadoras hace que existan más de los 80 ó 100 mil tipos de virus conocidos a finales del 2002[16], y que su impacto, cuando logran trascender, sea mucho mayor.

El virus informático es un programa que posee la capacidad de crear duplicados de sí mismo, en algunos casos introduciendo ligeras variaciones, y distribuirlos a través de un sistema. Para mantenerse ocultos, los virus se instalan en el interior de otros programas, no pudiendo vivir aislados. A veces, su objetivo es la destrucción de información; sin embargo, también producen simplemente efectos curiosos o visuales haciendo alusión a protestas[17].

Gusanos. Son programas que se autoduplican y autopropagan, en donde se consumen los recursos de la computadora, afectando el rendimiento y bloqueando los sistemas; la línea que los separa de los virus es muy delgada; la diferencia es que se pueden transmitir en sistemas como Unix, en sistemas que son más seguros.

Backdoors o puertas falsas. Son programas que permiten la entrada en el sistema, de manera que el usuario habitual del mismo no tenga conocimiento de este ataque.

Caballos de Troya. Se utilizan normalmente para instalar puertas traseras que causan vulnerabilidades y facilidades a hackers[18].

---

15 Tulloch, Mitch. Microsoft Encyclopedia of Security, Microsoft Press, US, 2003, Pág. 290-350
16 Symantec 2002
17 Nombela Juan . Seguridad Informática, Ed. Paraninfo 1996. Pág. 45-50
18 Strebe Matthew. Network Security Foundations. Ed. Sybex, 2004, Pág. 30

Ataques al personal. Aunque lo parezca, no consiste en perseguir con un cuchillo a los administradores. Se suele conocer más como ingeniería social. Consiste realmente en mantener un trato social con las personas que custodian datos. Indagar en sus costumbres o conocerlas más profundamente para perpetrar posteriormente un ataque más elaborado. La ingeniería social incluye desde suplantación de identidades confiables, hasta la búsqueda en papeleras y basuras de información relevante.

3.6 ALGUNOS MÉTODOS DE PROTECCIÓN

Por regla general, se deben generar en primer plano políticas en una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda. (pro actividad)

A continuación se describen algunos métodos:

1. Sistemas de detección de intrusos. Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, basándose en la información con la que han sido previamente alimentados.

2. Sistemas orientados a conexión de red. Monitorear las conexiones de red que se intentan establecer con una red o un equipo en particular, siendo capaces de efectuar una acción con base en métricas, como: origen de la conexión, destino de la conexión, servicio solicitado, etc. Las acciones que pueden emprenderse suelen ir desde el rechazo de la conexión, hasta alertar al administrador vía correo electrónico o vía pager. En esta categoría están los firewalls y los wrappers.

3. Sistemas de análisis de vulnerabilidades. Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que pueden ser utilizados tanto por personas autorizadas, como por personas que busquen acceso no autorizado al sistema.

4. Sistemas de protección a la privacidad de la información. Herramientas que utilizan criptografía para asegurar que la información sólo es visible a quien tiene

autorización de verla. Su aplicación es principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas podemos situar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los certificados digitales tipo X.509.

5. Sistemas de protección a la integridad de información. Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest 5 (MD5) o Secure Hash Algorithm 1 (SHA-1), o bien sistemas que utilizan varios de ellos como Tripwire[19].

3.7 ALGUNOS CRITERIOS DE SEGURIDAD

Ya que las empresas crecen, se hace necesario establecer medidas preventivas a la informática, es fundamental establecer y determinar características de la seguridad, a continuación se detallan algunas de éstas.

Confidencialidad. La información está disponible sólo para el usuario autorizado a manejarla, pero puede ser accesible por atacantes, si bien no sabrán interpretarla o entenderla de primera instancia, este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Integridad. Garantizar que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor. Garantiza que la información no sea falsa y que se ha mantenido intacta.

Autenticidad. Asegurar el origen y destino de la información.

No repudio. Quien envía información no puede alegar que no envió los datos.

Disponibilidad. Asegura que el sistema de computación esté disponible a las partes autorizadas siempre que sea requerido, y no existan problemas de caídas, cuelgues o funcionamiento dudoso de las máquinas que prestan los servicios.

Control de acceso. Se utiliza para evitar el uso no autorizado de recursos.

Normalmente, los mecanismos que pueden contar con alguna de estas características proporcionan más de una al mismo tiempo; por ejemplo, control de acceso y autenticidad están muy relacionados.

19 Tulloch, Mitch. Microsoft Encyclopedia of Security. Microsoft Press, US, 2003, Pág 290-300

Con los puntos anteriores se puede asegurar la invulnerabilidad de la información, pero no al 100 %, pues existe el problema de los protocolos. Esto es, los pasos que hay que tomar entre dos interlocutores para establecer una comunicación segura. Aún si los datos están cifrados y las partes confían una en la otra, si el protocolo no está bien diseñado, la comunicación puede ser interceptada, modificada e interrumpida.

3.8 ARQUITECTURA DE LA RED

En este apartado se presenta cómo se inicia o prepara el estudio de las redes, ya que al ser un conjunto particularmente complejo, necesita una estructuración que permita descomponer el sistema en sus elementos directamente realizables. Se introduce así el modelo de referencia para la interconexión de sistemas abiertos (OSI, Open Systems Interconection)[20]. Se trabaja sobre la capa de presentación, que se encarga en mayor medida de la seguridad y cifrado de los datos intercambiados.

Estructuras en niveles

El modelo OSI[21] mostrado en la Figura 3.1 de ISO (International Standards Organization) surge en el año 1984, ante la necesidad imperante de interconectar sistemas de procedencia diversa, cada uno de los cuales empleaban sus propios protocolos para el intercambio de señales. El término abierto se seleccionó con la idea de realizar la facilidad básica del modelo que dio origen al mismo, frente a otros modelos propietarios, por lo tanto, cerrados.

El modelo OSI está compuesto por una pila de siete niveles o capas, cada uno de ellos con una funcionalidad específica, para permitir la interconexión e interoperabilidad de sistemas heterogéneos. La utilidad radica en la separación que en él se hace de las distintas tareas que son necesarias para comunicar datos entre dos sistemas independientes. Es importante señalar que este modelo no es una arquitectura de red en sí mismo, ya que no se especifican, los servicios y protocolos que se utilizarán en cada nivel, sino que solamente indica la

20 Stewart James Michael and Chapple Mike. CISSP: Certified Information Systems Security Professional Study Guide, Second Edition, US,
21 Groth David and Skandier Toby. Network+ Study Guide. Ed. Sybex, Fourth Edition (N10-003), 2005, US, Chapter 2

funcionalidad de cada uno de ellos. Sin embargo, ISO también ha generado normas para la mayoría de los niveles, aunque éstas no forman parte del modelo OSI, habiéndose publicado todas ellas como normas independientes.

Núm	Nivel	Función
7	Aplicación	Datos Normalizados
6	Presentación	Interpretación de los datos
5	Sesión	Dialogos de control
4	Transporte	Integridad de los mensajes
3	Red	Encaminamiento
2	Enlace	Detección de errores
1	Físico	Conexión de equipos

Figura 3.1 Capas del Modelo OSI

3.9 SNIFFERS, MONITORES DE RED Y OTRAS HERRAMIENTAS

Un sniffer[22] es un proceso que identifica el tráfico que se genera en la red a nivel de enlace; de este modo se puede leer toda la información que circule por el tramo o segmento de red en el que se encuentre. Por este método se pueden capturar claves de acceso, datos que se transmiten, números de secuencia, etc.

Un analizador de protocolos es un sniffer al que se le ha añadido funcionalidad suficiente como para entender y traducir los protocolos que se están hablando en la red. Debe tener suficiente funcionalidad como para entender las tramas de nivel de enlace y los paquetes que transporten.

Normalmente, la diferencia entre un sniffer y un analizador de protocolos, es que el primero no muestra claves de acceso.

Información en nivel de enlace

Quiere decir que el sniffer se dedica a leer tramas de red, por lo que los datos que obtendremos de él serán tramas que transportan paquetes (IP, IPX, etc.). En estos paquetes se incluyen los datos de aplicación, entre ellos claves de acceso.

Estos programas ponen al menos una interfaz de red (o tarjeta de red) en modo promiscuo; es decir, que al menos una de las interfaces de red de la máquina está programada para leer toda la información que transcurra por el tramo de red al que esté conectado, y no solamente los paquetes que son dirigidos a él.

22 Tulloch , Mitch. Microsoft Encyclopedia of Security. Microsoft Press, 2003, US, Pág 252-270

Caso de vulnerabilidad (red con topología de estrella)

Cualquier tipo de red basada en bus o anillo lógico es vulnerable. Aunque los cables se envíen a un concentrador hub, haciendo que la topología física sea de estrella, si la topología lógica de la red es en bus o en anillo, las tramas podrán escucharse desde cualquier host conectado al concentrador.

En general, IEEE 802.3 (Ethernet), 802.4 (Token Bus) [23], 802.5 (Token Ring) [24], Ethernet 2, etc., (Token Bus es un protocolo para redes de área local análogo a Token Ring, pero en vez de estar destinado a topologías en anillo está diseñado para topologías en bus), suelen ser vulnerables, con la salvedad de que algunos concentradores de nueva generación aíslan el tráfico entre hosts conectados a una misma red; por lo que en estas redes la utilización de sniffers es poco menos que inútil (excepto en ciertos casos donde la carga de la red obliga al concentrador a unir varios buses lógicos en uno físico; esta salvedad puede no cumplirse dependiendo del concentrador utilizado).

Uso inadecuado de herramientas de monitoreo

La forma más común de saber si una interfaz de red está en modo promiscuo consiste en ejecutar (en máquinas UNIX) el programa ifconfig[25] de la siguiente forma:

- $ifconfig –a [Muestra el estado de las tarjetas de red. La salida sería similar a ésta]
- eth0 Link Encap: 10Mbps Ethernet HWaddr: xx:xx:xx:xx:xx:xx
- inet addr: a.b.c.d Bcast: a.b.c.f Mask: m.m.m.m
- UP BROADCAST RUNNING **PROMISC** MULTICAST MTU:1500 Metric:1
  - RX packets: 0 errors:0 dropped:0 overruns:0
  - TX packets:0 errors:0 dropped:0 overruns:0
  - Interrupt:15 Base Address:0x300

El problema de esta solución es que se necesita tener acceso root a todas las máquinas que deben comprobarse. Otra opción sería hacer un crontab que

23 Tulloch, Mitch. Microsoft Encyclopedia of Security. Microsoft Press, 2003, US, Pág 130-145
24 Tulloch , Mitch. Microsoft Encyclopedia of Security. Microsoft Press, 2003, US, Pág. 215-245
25 Tulloch , Mitch. Microsoft Encyclopedia of Security. Microsoft Press, 2003, US, Pág. 215-245

compruebe el estado cada cierto tiempo, sin embargo un cracker con acceso al sistema puede ver los trabajos en crontab y deshabilitar esta verificación.

Por lo que es necesario tener presente todos los puntos que intervienen en la seguridad informática y la labor que se debe llevar a cabo para convencimiento de la alta dirección sobre la importancia de la inversión, el factor humano, la capacitación, los riesgos que tiene la organización y la información por una mala visión de las necesidades del área de informática.

CAPÍTULO ?V

SEGURIDAD Y FIREWALL

4.1 CONCEPTOS TEÓRICOS

Un firewall[26] o corta fuego es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes o más[27]. De una forma más clara, podemos definir un firewall como cualquier sistema, desde un simple router hasta varias redes en serie, utilizado para separar, en cuanto a seguridad se refiere, una máquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad. El espacio protegido, denominado perímetro de seguridad, suele ser propiedad de la misma empresa, y la protección se realiza contra una red externa, no confiable, llamada zona de riesgo.

Evidentemente la forma de aislamiento más efectiva para cualquier política de seguridad consiste en el aislamiento físico, es decir, no tener conectada la máquina o la subred a otros equipos o a Internet, Figura 4.1. Sin embargo, en la mayoría de organizaciones o empresas, los usuarios necesitan compartir información con otras personas situadas en muchas ocasiones a distancia, por lo que no es posible un aislamiento total. El punto opuesto se considera en una conectividad total con la red, Figura 4.2, lo que desde el punto de vista de la seguridad es muy problemático: desde cualquier parte del mundo, puede potencialmente tenerse acceso a nuestros recursos. Un término medio entre ambas aproximaciones consiste en implantar cierta separación lógica mediante un firewall, Figura 4.3.

Antes de hablar de un firewall es casi obligatorio dar alguna definición y características del funcionamiento; ya que una máquina o host se considera un sistema especialmente asegurado, pero en principio vulnerable a todo tipo de ataques por estar abierto a Internet, que tiene como función el punto de contacto a los usuarios de la red interna de una organización con otro tipo de redes. El firewall filtra tráfico de entrada y salida, también esconde la configuración de la red hacia fuera.

Por filtrado de paquetes entendemos la acción de denegar o permitir el flujo de tramas entre dos redes (por ejemplo la interna, protegida con el firewall y el resto

26 Strebe Matthew. Network Security Foundations. Sybex, 2004, Chapter 4
27 Cheswick William and Bellovin Steven M. Firewalls and Internet Security. Addison-Wesley Publishing, US, January 1994,

de Internet) de acuerdo a unas normas predefinidas; aunque el filtro más elemental puede ser un simple router, trabajando en el nivel de red del protocolo OSI; esta actividad puede realizarse además en un puente o en una máquina individual. El filtrado también se conoce como screening y a los dispositivos que lo implementan se les denomina choke; éste puede ser la máquina en donde está instalado el firewall o un elemento diferente.

Un proxy es un programa (trabajando en el nivel de aplicación de OSI) que permite o niega el acceso a una aplicación determinada entre dos redes. Los clientes proxy se comunican sólo con los servidores proxy, que autorizan las peticiones y las envían a los servidores reales, o las deniegan y las devuelven a quien las solicitó.

Físicamente, en casi todos los firewalls existe al menos un simple router filtrador de paquetes también conocido como choke, desde el punto de vista lógico, en el firewall suelen existir servidores proxy para las aplicaciones que han de atravesar el sistema y que se sitúan habitualmente en el host.

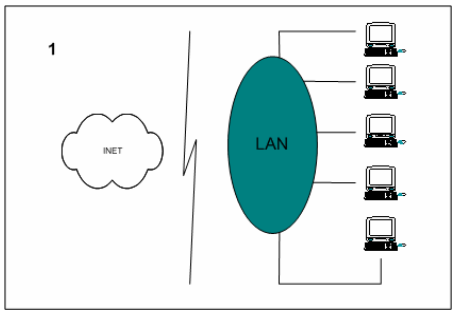


Figura 4.1 Aislamiento

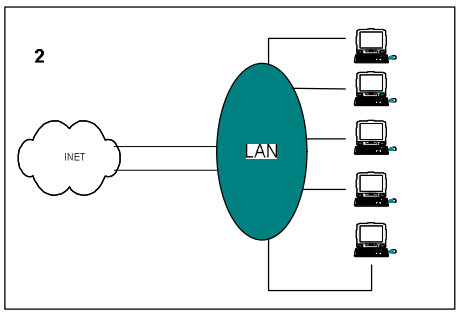


Figura 4.2 Conexión total

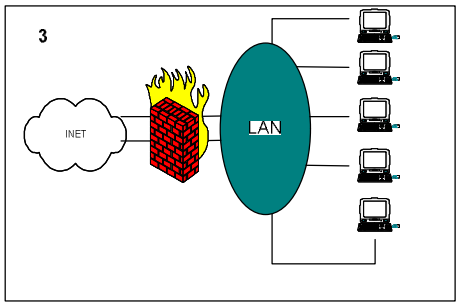


Figura 4.3 Firewall que está entre la zona de riesgo y el perímetro de seguridad

También se implementa en el firewall un mecanismo de filtrado de paquetes, y en alguno de los dos elementos se suele situar otro mecanismo para monitorear y detectar la actividad sospechosa.

Hablaremos de los firewall más habituales y de sus características, así como de las posibles políticas de seguridad que se pueden implantar. Posteriormente, comentaremos aspectos de algunos de los firewalls más utilizados hoy en día, como Firewall-1, Cisco PIX Firewall.

Firewall-1. Es el firewall más utilizado cuando de acceder a Internet se requiere, ya que se ejecuta sobre diferentes sistemas Unix (Solaris, AIX, Linux y HP-UX) de igual forma sobre Windows, como en denominadas "cajas negras", desarrolladas por Nokia que tienen un sistema operativo propio (IPSO) basado en FreeBSD. Como una característica importante está el hecho de incorporar una nueva arquitectura: la inspección con estado (starefull inspection). Cuenta con un módulo llamado Inspección en el interior del sistema operativo, por lo que se trabaja en un nivel bajo de la capa OSI, se puede interceptar y analizar todos los paquetes antes de que lleguen al resto del sistema, por lo que se garantiza que ningún paquete es procesado por ninguno de los protocolos superiores hasta que el firewall comprueba que no viola la política de seguridad definida en el firewall.

El Firewall-1 es capaz de analizar la información de una trama en cada uno de los siete niveles OSI y a la vez analizar información de estado registrada de anteriores comunicaciones; el firewall entiende la estructura de los diferentes protocolos TCP/IP, incluso de los ubicados en la capa de aplicación, de forma que el módulo de inspección extrae la información relevante de cada paquete para construir tablas dinámicas que se actualizan constantemente, tablas que el firewall utiliza para analizar comunicaciones posteriores. En éste se implantan las políticas de seguridad definidas en cada organización mediante un sencillo lenguaje denominado INSPECT, también diseñado por Check Point Software Technologies; desde una cómoda interfaz se genera un script en este lenguaje, que se compila y se inserta. La anterior característica es fundamental en el funcionamiento de este tipo de firewall, lo cual hace que sea adquirido por empresas.

Firewall Cisco Secure PIX. Una característica principal es la velocidad de proceso. La arquitectura de PIX se construye alrededor del motor de seguridad de ASA que realiza la inspección y mantiene la información del estado de la sesión y maneja la traducción de red.

El firewall de PIX permite, por defecto, cualquier sesión o flujo de datos al paso de la seguridad más alta que interconecta una interfaz con un nivel de la seguridad más baja sin restricciones. Ésta es una característica válida en proceso de hoy de la seguridad cuando un usuario ya comprometido, puede iniciar sesiones de salida e infectar a otros usuarios. Es recomendado fuertemente para inhabilitar esta característica usando el acceso-lista en todas las interfaces y para definir el tráfico legítimo mientras se transfiere cualquier cosa.

Los firewalls son cada vez más necesarios en nuestras redes, pero los expertos recomiendan que no se usen en lugar de otras herramientas, sino junto a ellas; cualquier firewall, desde el más simple al más avanzado, presenta dos graves problemas de seguridad: por un lado, centralizan todas las medidas en un único sistema, de forma que si éste se ve comprometido y el resto de nuestra red no está lo suficientemente protegido, el atacante consigue amenazar a toda la subred simplemente poniendo en jaque a una máquina. El segundo problema, relacionado con éste, es la falsa sensación de seguridad que un firewall proporciona, generalmente un administrador que no disponga de un firewall va a preocuparse de la integridad de todas y cada una de sus máquinas, pero en el momento en que instala el firewall y lo configura asume que toda su red es segura, por lo que se suele descuidar enormemente la seguridad de los equipos de la red interna. Esto es un grave error, ya que en el momento que un hacker acceda a nuestro firewall (es un sistema muy expuesto a ataques externos) automáticamente va a tener la posibilidad de controlar toda nuestra red.

Un firewall evidentemente no protege contra ataques que no pasan por él: esto incluye todo tipo de ataques internos dentro del perímetro de seguridad, pero también otros factores que a priori no deberán suponer un problema. El típico ejemplo de estos últimos son los usuarios que instalan sin permiso, sin conocimiento del administrador de la red, y muchas veces sin pensar en sus

consecuencias, un simple módem en sus pcs o estaciones de trabajo; esto, tan habitual en muchas empresas, supone la violación y la ruptura total del perímetro de seguridad, ya que posibilita accesos a la red no controlados por el firewall. Otro problema de sentido común es la reconfiguración de los sistemas al pasarlos de una zona a otra con diferente nivel de seguridad, por ejemplo al mover un equipo que se encuentra en el área protegida a la DMZ (zona desmilitarizada). Este acto que en ocasiones no implica ni tan siquiera el movimiento físico del equipo, sino simplemente conectarlo en una toma de red diferente, puede ocasionar graves problemas de seguridad en nuestra organización, por lo que cada vez que un cambio de este estilo se produzca no sólo es necesaria la reconfiguración del sistema, sino la revisión de todas las políticas de seguridad aplicadas a esa máquina.

4.2 DEFINICIÓN DE FIREWALL

Un corta fuegos o firewall es un sistema de defensa basado en el hecho de que todo tráfico de entrada o salida a la red debe pasar obligatoriamente por un sistema de seguridad capaz de autorizar, denegar y tomar nota de aquello que ocurre en la red.

Aunque hay programas que se venden bajo el término de firewall, éstos consisten en un conjunto de medidas de hardware y software destinadas a asegurar una instalación de red.

4.3 FUNCIONAMIENTO DE UN FIREWALL

Un firewall normalmente trabaja en los niveles 3 (red) a 7 (aplicación) del modelo OSI. Sus funciones son básicamente las siguientes:

1. Llevar la cuantificación de las transacciones realizadas en la red e intranet.
2. Filtrar accesos no autorizados a máquinas (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de transporte, sesión, presentación y aplicación).
3. Puede delimitar el ancho de banda por servicio y puerto.

4. Alertar en caso de ataques o comportamiento extraño de los sistemas de comunicación.
5. Auto reconfigurarse en el instante del intento de vulnerabilidad.

Las características anteriores pretenden facilitar la selección del firewall que se apegue a nuestras necesidades, siempre dependiendo de la función que deseamos dentro de la empresa.

4.4 TIPOS DE FIREWALL

Cualquier firewall puede clasificarse dentro de uno de los tipos siguientes (o como una combinación de los mismos):

Filtros (packet filters). Consiste en filtrar paquetes dejando pasar por el tamiz únicamente cierto tipo de tráfico. Estos filtros pueden implantarse a partir de routers. Por ejemplo, en un firewall Cisco PIX podemos definir las listas de acceso (access-lists) asociadas a cada una de las interfaces de red disponible.

Problemas. No son capaces de discernir si el paquete cuya entrada se permite incluye algún tipo de datos “malicioso". Además, cualquier tipo de paquetes no permitido puede viajar en el interior de tráfico.

Proxy (circuit gateways). En este caso la pasarela actúa del mismo modo que un simple cable, vía software conectando nuestra red interna con el exterior. En general, se requiere que el usuario esté autorizado para acceder al exterior o interior y que tenga una cuenta de salida en el proxy.

Aplicaciones gateway. Estas pasarelas se ocupan de comprobar que los protocolos a nivel de aplicación (ftp, http, etc) se están utilizando de forma correcta, sin tratar de explotar algunos problemas que pudiese tener el software de red.

Problemas. Deben estar actualizados; de otro modo no habría forma de saber si alguien está tratando de atacar nuestro sistema.

4.5 DEFICIENCIAS DE UN FIREWALL

Las redes firewall no pueden protegernos de ataques que se producen por causas distintas a dicha red. Muchas empresas que cuentan con conexiones de Internet no tienen coherencia a la hora de protegerse de invasiones a través del módem.

Es incongruente poner puertas traseras después de haber invertido mucho dinero en un firewall, es como si pusiéramos una puerta de acero de seis pulgadas de espesor si se vive en una casa de madera. Sin embargo, es común que se invierta en comprar redes firewall, descuidando después las numerosas aberturas por las que se puede colar un intruso (lo que se llaman "back-doors" o "puertas traseras").

Para que un firewall tenga una efectividad completa, debe ser una parte consistente en la arquitectura de seguridad de la empresa. Por ejemplo, si se tiene conexión directa a Internet, a los sistemas o a los datos realmente secretos deberían ser aislados del resto de la red corporativa. Otra cosa contra la que los firewalls no pueden luchar, son los ataques internos que haya en la propia organización. Es evidente, que de nada sirve que se instale un firewall para proteger nuestra red, si existen personas dentro de la misma que se dedican a traspasar información a través de algún dispositivo de almacenamiento, como son memorias USB, CD u otro, a empresas espías que pueden repercutir en el futuro de la compañía.

4.6 ADQUISICIÓN DE UN FIREWALL

Hay puntos básicos que hay que tratar en el momento en que una persona toma la responsabilidad o se la asignan, de diseñar, especificar e implantar o supervisar la instalación de un firewall.

El primero, y más importante, es reflejar la política con la que la compañía u organización quiere trabajar con el sistema, esto es, ¿se destina el firewall para denegar todos los servicios excepto aquellos críticos para la misión de conectarse a la red? o ¿se destina el firewall para proporcionar un método de medición y auditoría de los accesos no autorizados a la red?, entre otras responsabilidades.

El segundo es: ¿Qué nivel de vigilancia, redundancia y control necesitamos? Hay que establecer un nivel de riesgo aceptable para resolver el primer asunto tratado. Para ello, se puede establecer una lista de comprobación o revisión de lo que debe ser vigilado, permitido y denegado. En otras palabras, se empieza buscando una serie de objetivos y entonces se combina un análisis de necesidades con una estimación de riesgos para llegar a una lista en la que se especifique lo que realmente se puede implantar.

El tercer punto es financiero. Dado a que en las empresas una premisa es la inversión que se realiza es importante cuantificar y proponer soluciones en términos de cuánto cuesta comprar la solución. Por ejemplo, un producto completo de red firewall puede costar más de 100,000 dólares. Pero este precio se trata de una solución de alta resolución final. Si no se busca tanta resolución es indispensable evaluar otras alternativas. A veces lo necesario no es gastar mucho dinero, sino no perder tiempo en evaluar las necesidades y encontrar un firewall que se adapte a ellas.

En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios proxy tales como telnet, ftp, news, etc., o bien, colocar un router a modo de filtro, que permita comunicaciones con una o más máquinas internas. Hay sus ventajas e inconvenientes en ambas opciones; con una máquina proxy se proporciona un gran nivel de auditoría y seguridad, en cambio se incrementan los costos de configuración y se decrementa el nivel de servicio que puede proporcionar.

4.7 SERVIDORES PROXY

Un servidor proxy hace referencia al nombre de "gateway", puerta de comunicación o "forwarder", agente de transporte. Es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los proxys se utilizan frecuentemente, como sustitutos de routers controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes. Éstos contienen logines auxiliares y soportan la autenticación de usuarios. Por otro lado, un proxy debe entender el protocolo de la aplicación que está siendo usada, aunque también pueden implantar protocolos específicos de seguridad, por ejemplo: un proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente.

Un conjunto muy conocido de servidores proxy son los TIS Internet Firewall Toolkit "FWTK", que incluyen proxy para telnet, rlogin, FTP, X-Windows, http/Web, y NNTP/Usenet news. La herramienta socks es un sistema proxy genérico que puede ser compilado en una aplicación cliente para hacerla trabajar a través de un firewall.

4.8 TIPOS BÁSICOS DE REDES FIREWALL

Conceptualmente, existen dos tipos de firewall:

1. A nivel de red
2. A nivel de aplicación

Las últimas tecnologías no aportan claridad para distinguir los dos tipos de redes, hasta el punto que no está claro cuál es mejor y cuál es peor. Pero en cualquier caso, se deberá prestar atención y poner mucho cuidado a la hora de instalar la que realmente se necesita en nuestra organización.

Los firewalls a nivel de red generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" firewall a nivel de red, particularmente, desde el momento que no puede tomar decisiones sofisticadas en relación con quién está comunicando un paquete ahora o desde dónde está llegando en este momento. Los firewall que trabajan en capa de red se han sofisticado ampliamente y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellas, así como, asignar ancho de banda por servicio y los contenidos de algunos datagramas. Un aspecto importante que distingue a los firewall que trabajan en capa de red es que dirigen el tráfico a través de ellos mismos, de forma que un usuario cualquiera necesita tener un bloque válido de dirección IP asignado.

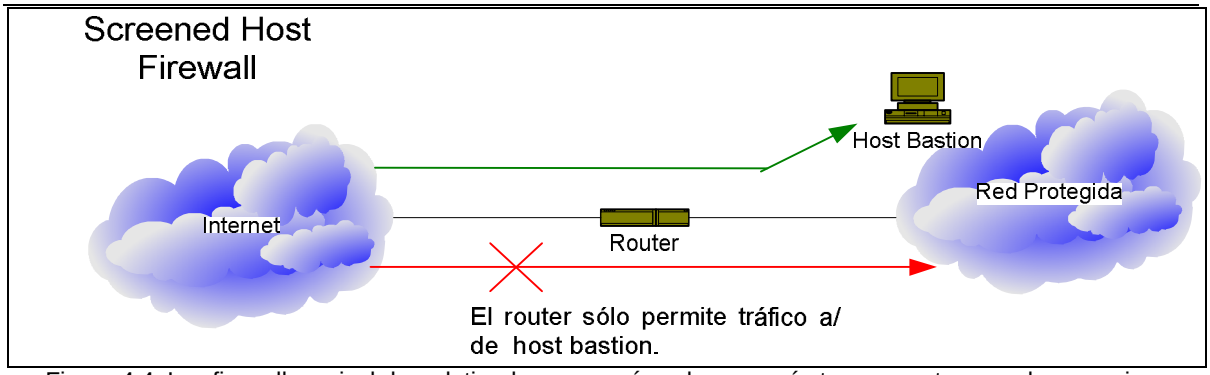


Figura 4.4 Los firewalls a nivel de red tienden a ser más veloces y más transparentes para los usuarios

En la Figura 4.4 se representa un firewall a nivel de red llamado "Screened Host Firewall". En dicho firewall, se accede a y desde un único host, el cual es

controlado por un router operando a nivel de red. El host es como un bastión, dado que está muy defendido y es un punto seguro para refugiarse contra los ataques.

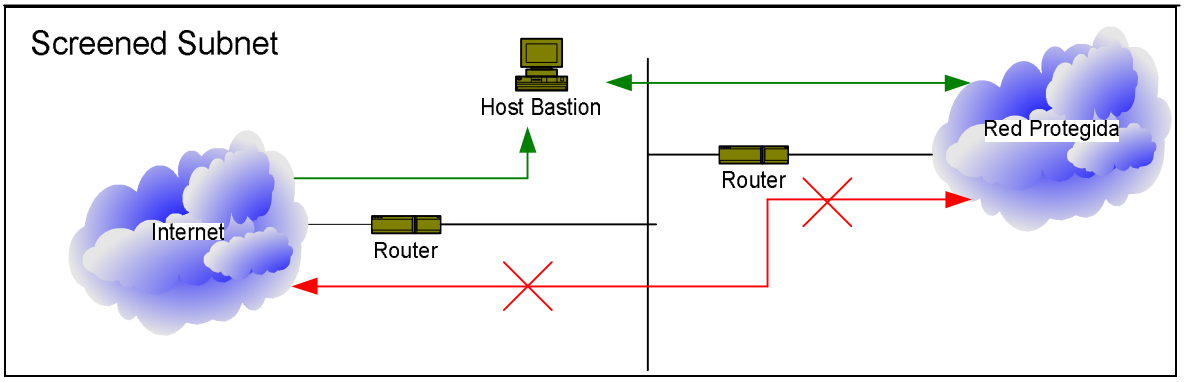


Figura 4.5 El ruteador sólo permite tráfico a/de la red DMZ

En el ejemplo de la Figura 4.5 se representa un firewall a nivel de red llamado "Screened Subnet Firewall". En dicho firewall se accede a y desde el conjunto de la red, la cual es controlada por un router operando a nivel de red. Es similar al firewall indicado en el ejemplo anterior, salvo que ésta sí es una red efectiva de hosts protegidos.

Los firewalls que trabajan en nivel de aplicación son, generalmente, hosts que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellos. El firewall a nivel de aplicación se puede usar como traductor de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeros a nivel de aplicación eran poco manejables y fáciles de entender para los usuarios finales, pero los modernos firewalls a nivel de aplicación ya no los son. Tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto los hace diferenciarse de los firewalls a nivel de red.

Cuando se busca que un host de alta seguridad corra bajo software del tipo proxy, se requiere de dos interfaces de red (uno a cada red), las cuales bloquean todo tráfico que pasa a través de la red, como se muestra en la Figura 4.6.

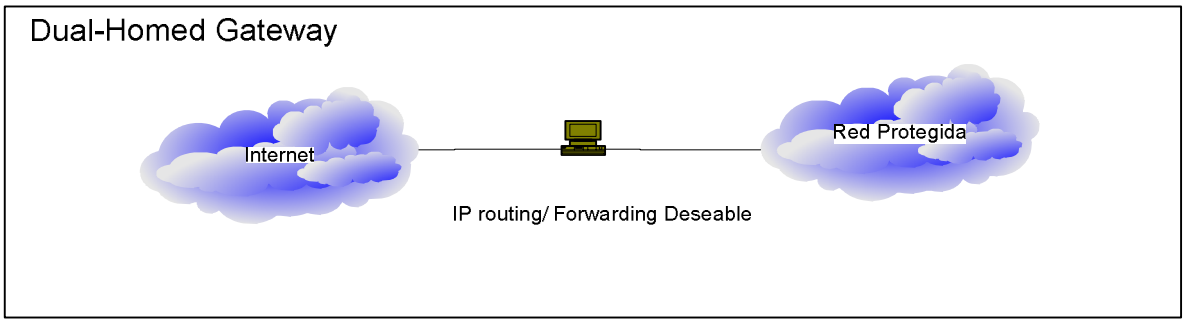


Figura 4.6 Firewall a nivel aplicación

4.9 TENDENCIA DE LOS FIREWALLS

Se encuentra a medio camino entre los firewalls a nivel de red y los de a nivel de aplicación. El resultado final que se obtiene será un sistema rápido de protección de paquetes que conecte y audite datos que pasan a través de él. Cada vez más, los firewalls (tanto a nivel de red como de aplicación), incorporan encriptación de modo que pueden proteger el tráfico que se produce en Internet. Estos mismos con encriptación extremo-a-extremo (end-to-end), se pueden usar por organizaciones con múltiples puntos de conexión a Internet, para utilizar Internet como una "central privada" donde no sea necesario preocuparse de que los datos o contraseñas puedan ser capturados.

4.10 SERVICIOS Y PUERTOS

Un firewall bloquea los servicios basados en datagramas (una parte de cabecera y en una parte de datos cuyo tamaño es variable) que no hagan uso de autenticación en UDP no cifrados y todos los servicios basados en TCP que no se consideren necesarios.

A continuación, se presenta una lista de servicios que son vulnerables cuando se accede a Internet, su descripción y posibles problemas que pueden surgir con cada uno de ellos. Ciertos servicios de esta lista sólo se han definido bajo TCP y sin embargo tienen asignado también un puerto UDP.

echo (7/tcp,udp). Se utiliza únicamente para depuración. Sin embargo, el atacante puede realizar "labores de depuración" creando bucles en la red a partir de este puerto.

Systat (11/tcp/udp). Muestra información acerca de usuarios conectados, carga del sistema, procesos en funcionamiento, etc.

Chargen (19/tcp,udp). Se utiliza únicamente para depuración. Basta con enviar un paquete a este puerto aparentemente originado en el puerto de echo (7/udp) para provocar un bucle en la red.

Telnet (23/tcp,udp). Vulnerable a "toma de sesiones". Es preferible utilizar en su lugar otras soluciones como SSH (Secure Shell).

Smtp (25/tcp,udp). Históricamente la mayoría de las entradas en hosts han venido a través de este puerto. Se debe filtrar este puerto y mantener siempre la última versión estable conocida de cualquier programa de correo, especialmente si trabajamos con sendmail.

Time (37/tcp,udp). Devuelve la hora del sistema en un formato legible para la pc (4 bytes más o menos). Puede ser accedido tras un ataque vía ntp (123/tcp,udp).

Nameserver (42/tcp,udp). Si dispone de una red privada, debe instalar un servidor de nombres para ella. Se debe bloquear el acceso a dicho servidor desde el exterior. En este caso, puede cortar sin excesivos problemas el acceso al DNS sobre UDP.

Tftp (69/tcp,udp). Falta de autenticación. Bloquear si no se dispone de máquina alguna con arranque remoto.

Private dialout (75/tcp,udp). Si encontramos una traza de este puerto en los diarios del sistema (logs), en el mejor de los casos estaremos siendo analizados por un scanner de puertos.

Algunos servicios que se sugiere deben ser bloqueados.

Finger (79/tcp,udp). Puede obtenerse información acerca de usuarios concretos, información que puede utilizarse para adivinar claves de acceso, bloquear o sustituir por una política coherente de asignación de direcciones de correo (Juan .... - - -> juan@host.com) y un mensaje advirtiendo de dicha política.

Http (80/tcp,udp). Los servidores web son cada vez más complejos y permiten demasiadas conexiones y tráfico de paquetes. Conviene redirigir el acceso a un puerto no privilegiado en máquinas Unix. De ser posible, se deben utilizar

servidores http específicos para la tarea a realizar (servir archivos, acceso a bases de datos, etc).

Npp (92/tcp,udp) - [Network Printing Protocol] Si no se quiere imprimir documentos ajenos y hay que bloquear.

Objcall (94/tcp,udp) - [Tivoli Object Dispatcher]. Utilizado por la herramienta de gestión de redes tivoli. Aplicar las mismas precauciones que con SNMP.

Sunrpc (111/tcp,udp). Especialmente peligroso sobre UDP. No autentica origen, y es la base para otros servicios como NFS.

Auth (113/tcp,udp). No debería permitirse obtener información acerca de puertos privilegiados. No se utiliza más que en Unix.

Ntp (123/tcp,udp) [Network Time Protocol]. Se utiliza para sincronizar los relojes de las máquinas de una subred. Un ejemplo de ataque clásico consiste en enviar paquetes a este puerto para distorsionar los logs de la máquina.

Snmp (161/tcp,udp). Se puede obtener mucha información a través de este servicio; como por ejemplo, estado de las interfaces de red, conexiones concurrentes en la máquina, etc. Hay que bloquear.

Snmp-trap (162/tcp,udp). Traps de SNMP. A través de este puerto se realizan solicitudes que pueden cambiar la configuración del host. Hay que bloquear.

Irc (194/tcp,udp). No es peligroso en sí; sin embargo, sus usuarios suelen divertirse atacando los hosts de otras personas con el fin de echarlos cuando no pueden hacer uso de la orden 'kick'. Generalmente conviene bloquear los puertos 6666, 6667 y 6668 ya que son a los que se enganchan los servidores de Irc.

Biff (512/udp). Notifica de la llegada de correo. Buen candidato para posibles desbordamientos de buffer, o simplemente para obligar a abandonar la sesión a un usuario debido a la llegada masiva de mensajes de correo (biff suele funcionar incluso con mesgn). Hay que bloquear.

login (513/tcp) – rlogin. Hay que bloquear.

cmd (514/tcp). Similar a exec (512/tcp), mismas precauciones. Hay que bloquear.

syslog (514/udp). Bloquear, a menos que existan suficientes razones como para mantenerlo. Suele atacarse para corromper los diarios (logs) del sistema con entradas falsas.

router (520/tcp,udp). Local routing process. Hay que bloquear.

En la mayoría de los equipos con sistema operativo Unix se puede encontrar esta entrada en /etc/services. Ya que está dado de alta y es un puerto no privilegiado es un buen lugar para una puerta trasera.

4.11 FILTRADO DE PAQUETES

Consiste en una dupla <regla,acción> aplicada a los paquetes que circulan por una red. Generalmente, estas reglas se aplican en los niveles OSI de red, transporte y sesión, definiendo mecanismos mediante los cuales se niega o se otorga el acceso a determinados servicios.

El mejor sitio para instalar un filtro de paquetes es en el router que conecta nuestra red con el exterior tras el punto de demarcación interna. De este modo, ponemos una primera línea de defensa en nuestra red.

Un ejemplo es como se muestra en la Tabla 4.1:

Interfaz: internet-intranet1/eth0

Permitir	Servicio	Sentido	Hosts
si	todos	entrada/salida	todos
no	ftp	entrada	142.115.9.9/24
no	smtp	entrada/salida	142.115.9.8-14
si	smtp	entrada/salida	142.115.9.10

Tabla 4.1

En la mayoría de los routers y firewall estas reglas se verifican en el orden en el que aparecen en la tabla anterior hasta que puede aplicarse una de ellas. Esto obliga a ordenar las entradas en la Tabla 4.1, de tal forma que aparezca primero la de menor jerarquía de la aplicación y después la mayor.

Por ejemplo:

Interfaz: internet-intranet/eth0

Permitir	Servicio	Sentido	Hosts
si	smtp	entrada/salida	142.115.9.10
no	ftp	entrada	142.115.0/24
no	ftp-data	entrada	142.115.9.0/24
no	smtp	entrada/salida	142.115.9.8-14
si	todos	entrada/salida	todos

Tabla 4.2

En el ejemplo de la Tabla 4.2, se asume que se tiene un router sin ninguna lista de acceso (access-list) definida, y que se encuentra en funcionamiento con sus interfaces configuradas y activas.

Tras la conexión al router se debe entrar en modo preferente.

Si la clave que hemos introducido es correcta, en este momento podemos acceder a la configuración del router y modificarla. Sí el prompt puede cambiar, eso significa que hemos entrado de modo preferente.

Para modificar la configuración teclearemos la orden:

- En primer lugar se deben definir las listas de acceso para cada una de las interfaces (en nuestro caso sólo es uno).
- Debemos tener cuidado al introducir la lista ya que se puede cometer un error y podría hacer que no pudiésemos alcanzar el router al aplicar las listas de acceso (si accedemos vía telnet).

Para ello se tendrá que convertir la entrada en la Tabla 4.2, que habíamos preparado antes, como se muestra a continuación:

access-list lista_acceso {permit|deny} protocolo (tcp,udp,icmp...)
dir_ip mascara_red
[dir_ip mascara_red ...]
{eq, gt, lt} {puerto, servicio}
{in, out, any }
{established,...}

De este modo, la Tabla 4.1 quedaría de la siguiente forma:

Permitir	Servicio	Sentido	Hosts
si	smtp	entrada/salida	142.115.9.10

access-list 102 permit tcp 142.115.9.10 host eq smtp

O bien:

access-list 102 permit tcp 142.115.9.10 255.255.255.0 eq 25

Permitir	Servicio	Sentido	Hosts
no	ftp	entrada	142.115.9.0/24
no	ftp-data	entrada	142.115.9.0/24

access-list 102 deny tcp 142.115.9.0 255.255.255.0 eq 21

access-list 102 deny tcp 142.115.9.0 255.255.255.0 eq 22

Permitir	Servicio	Sentido	Hosts
no	smtp	entrada/salida	142.115.9.8-14

access-list 102 deny tcp 142.115.9.8-14 255.255.255.0 eq smtp

Permitir	Servicio	Sentido	Hosts
si	todos	entrada/salida	todos

access-list 102 permit tcp any host gt 0

Por lo tanto, tendremos la siguiente lista de acceso:

access-list	102	permit tcp 142.115.9.10 255.255.255.0	eq 25
access-list	102	deny tcp 142.115.9.0 255.255.255.0	eq 21
access-list	102	deny tcp 142.115.9.0 255.255.255.0	eq 22
access-list	102	deny tcp 142.115.9.8-14 255.255.255.0	eq smtp
access-list	102	permit tcp any host gt	0

Una vez definida y revisada la lista de acceso anterior, debemos aplicarla a una (o varias) de las interfaces.

De esta forma, el router ya está aplicando el filtro que le hemos especificado para cada uno de los paquetes que atraviesan la interfaz.

Un filtro puede fallar si:

- Las reglas definidas no son suficientes
- Las reglas son suficientes, pero su disposición no es correcta
- El filtro anula la tabla de routing de la máquina (poco probable)
- No permitimos que vengan de vuelta los paquetes de conexiones ya establecidas previamente

Sí después de haber realizado los filtros necesarios, se tienen problemas por una mala creación de lista de acceso, se puede tener como solución escribir la siguiente línea:

access-list 102 tcp permit dir_ip mascara_red gt 1023

Lo visto en el ejemplo anterior es una muestra de la forma que comúnmente se maneja en los accesos y políticas que se crean en los servidores Proxy, de donde se parte para crear las políticas en los firewalls. Por lo que es importante conocer la forma de creación de políticas cuando se administra un firewall, ya que puede creerse que es fácil; sin embargo, la identificación de éstas puede no serlo, ya que es frecuente contraponer las reglas, causando mayores problemas.

CAPÍTULO V
LEGISLACIÓN EN MÉXICO

5.1 LEGISLACIÓN EN MÉXICO

Lamentablemente, en la búsqueda de alguna ley que castigue cuando se lleve a cabo algún mal uso de la información y afecte a la seguridad informática y se realicé algún fraude informático, creación de virus informáticos, obtuve muy pocas referencias en México. Si bien en algunos países existen leyes que castiguen actos indebidos, también hay certificaciones e incluso ISO de seguridad.

En México estamos rezagados en la implantación de certificaciones que nos permitan cubrir con estándares de seguridad, aunque actualmente se cuenta con una ISO 17799 y a raíz de las reglas generales a las que deben sujetarse los prestadores de servicio publicadas en el Diario Oficial de la Federación,[28] derivada de estándares internacionales FIPS-140 nivel 3. En México se empieza a trabajar en este rubro e incluso para consultorías que brinden seguridad informática a empresas, puede ser requerido desde las características que debe cumplir el especialista, como es la certificación, experiencia, título, así como para el patrón de dicho empleado.

Por ejemplo, no existía alguien que regulara la consultoría en cuestiones de seguridad informática y a la problemática que se enfrenta un sistema de información desde una perspectiva global.

Hoy en día no se pueden dejar a un lado los problemas que se tienen en un mundo empresarial interconectado, que está expuesto a riesgos demasiado altos, sin saberlo. Por ello, son necesarias e importantes las certificaciones de seguridad, para el cumplimiento de los lineamientos internacionales, tales como:

1. GIAC-Global Information Assurance Certification.
2. GGSC GIAC Gold Standard Certificates.
3. GSLC-GIAC Security Leadership Certificat.

En este nuevo escenario, cualquier empresa es susceptible de verse involucrada en un incidente de seguridad informática y de requerir a alguien familiarizado con la

28 Diario Oficial de la Federación, México, D.F., 10 de agosto de 2004.

nueva forma de trabajar con niveles de seguridad, como lo presentamos en este trabajo.

Para evitar los incidentes de seguridad no es suficiente con adoptar medidas técnicas; además, es imprescindible tener en cuenta un amplio abanico de recomendaciones de tipo administrativo y de gestión adicional que se plantean en este trabajo, así como la evaluación de riesgos ya que puede ser amplia y compleja la administración de la seguridad informática.

En algunos países como Estados Unidos, España, entre otros, se aplica un análisis de seguridad ISO que les permite establecer un sistema de gestión de la seguridad de la información completa, estandarizada, efectiva y ordenada, así como identificar y determinar las necesidades de seguridad en una empresa.

Actualmente, en México no existen controles generalizados de “mejores prácticas” en la seguridad de la información, a excepción de la ISO 17799.

Es necesario contar con mejores prácticas que nos permita identificar los controles necesarios que involucren situaciones en que los sistemas de información se ven afectados en la industria y en el comercio. Las mejores prácticas pueden servir para facilitar el comercio de todo tipo en un entorno confiable y de alguna forma seguro, recordemos que no hay seguridad al 100 por ciento, ya que no podemos decir que una vez implantada la seguridad ahí termina el trabajo.

En México no estamos apegados a estándares internaciones que nos permitan estar alineados a certificaciones y a ISO internacionales.

Desde el 11 de septiembre de 2001 en Nueva York surgió un boom de la seguridad por los ataques a las Torres Gemelas, la informática y la competitividad fueron también algunas de ellas. Y es que la combinación de conjunción de seguridad-competitividad-informática definió el futuro de las empresas que desarrollan software y de los mercados que adquirirán mecanismos de seguridad. Por ejemplo, si el competidor de una empresa se certifica antes que la competencia, sencillamente éste puede ser un diferenciador en el mercado. Se considera necesaria la implantación de un sistema de seguridad integral y por supuesto la certificación en cuestiones de e-bussines. Simplemente porque como un despacho de abogados que lleva a cabo la fusión de dos empresas las consultorías deben

brindar y ejecutar auditorias apegadas a normas que estandaricen y brinden a las empresas las herramientas que les permitan cubrir los niveles de seguridad.

Sin embargo, mientras no existan los órganos que normen el cumplimiento de los mínimos niveles de seguridad en las empresas e instituciones, México será un país y un foco latente de fraudes.

Actualmente, en Estados Unidos una nueva ley está involucrando y brindando seguridad en los estados financieros conocida como Sarbanes Oxley, SOX. Las recientes reformas a marcos regulatorios en las organizaciones son resultantes de fraudes financieros como en los casos de Enron, WoldCom, GlobalCrossing. Respondiendo a estos fraudes, el congreso estadounidense aprueba el Acta de Ley Sarbanes Oxley (2002). Esta Acta de Ley afecta a los Estados Unidos, pero impacta igualmente a cualquier organización, la cual lidia comercialmente en este país o fuera de él. En esencia trabaja sobre procesos, apoyada en ISO 17799 y Cobit ISO 17799 que brindan y garantizan el cumplimiento de los estándares de confiabilidad utilizando sistemas y que transparente la información de los estados financieros. SOX al igual que ISO 9001:2000, requiere de auditorías (evaluaciones e inspecciones) en la efectividad de los procedimientos en materia contable, fiscal, financiera, sistemas, ética, en cada una de las actividades relevantes. Estas leyes requieren un estudio amplio que si bien en México no se apega a estos estándares hay que analizarlos y procurar implantar. Por lo que, actualmente la auditoría de sistemas ha tomado importancia para las empresas haciendo necesario el conocimiento de políticas, procedimiento y metodologías de seguridad.

La ISO 17799 es una guía que nos ayudará a cumplir estándares internacionales y hacer uso de tecnologías, por la complejidad de las organizaciones es común la creación de huecos en los sistemas, se incrementan los riesgos y es recomendable crear prácticas de seguridad ya que de lo contrario se pone en riesgo la información.

Dado que se pretende brindar la continuidad del negocio, es necesario contemplar 10 puntos que considera la ISO 17799 y que deben ser implantados.

A continuación, se enlistan diez puntos que se consideran necesarios en la normatividad internacional:

1. Continuidad del negocio

Hay que contrarrestar las interrupciones de las actividades productivas críticas del negocio. Evitar fallas mayores o desastres.

2. Generar sistemas de control de acceso

Actividades que deben llevarse a cabo en cualquier organización.

- Controlar el acceso a la información
- Prevenir los accesos no autorizados a sistemas de información
- Garantizar la protección de servicios de red
- Prevenir los accesos no autorizados a los servidores
- Detectar actividades no autorizadas
- Garantizar la seguridad de la información cuando se utilice equipo remoto.

3. Llevar a cabo un proceso de desarrollo y mantenimiento de sistemas

Garantizar que la seguridad del sistema contiene formas de monitoreo o de fácil obtención de información de la BD para prevenir pérdidas, abusos, modificaciones de los datos. Debe contener mecanismos para proteger la confidencialidad, autenticidad e integridad de la información. Los proyectos informáticos y sus actividades de soporte deberán ser conducidos de forma segura.

4. Seguridad física y ambiental

Hay que prevenir el acceso no autorizado a las instalaciones para evitar pérdida, robo, daño de los bienes y la interrupción de las actividades productivas.

5. Aplicar dentro de la empresa algún código de ética

- Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.
- Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.

- Maximizar la efectividad y minimizar las interferencias del sistema de auditoría en el proceso.

6. Seguridad del personal

Tratar de reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse que el personal esté consciente de las amenazas a la información y sus implicaciones. Deberán de apoyar la política corporativa de seguridad en contra de accidentes y fallas. A la vez deberán de aprender de estos incidentes.

7. Seguridad de la organización

- Hay que administrar la seguridad de la información dentro de la compañía.
- Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos accedidos por terceros (proveedores, clientes, etc.).
- Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros (out-sourcing).

8. Administración de las operaciones y equipo de cómputo

- Hay que asegurar la correcta operación de las instalaciones de procesamiento.
- Minimizar el riesgo de fallas en el sistema.
- Proteger la integridad del software y la información.
- Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.
- Asegurar la protección de la información en la red y de la infraestructura que la soporta.
- Prevenir el daño a los activos y procesos críticos del negocio.
- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre empresas.

9. Clasificación y control de activos

Fijarse la meta de tener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

10. Políticas de seguridad

Hay que proveer la directriz y el soporte de la dirección general de la empresa para la seguridad de la información.

El mejor punto de partida es realizar un análisis de la posición y situación de la empresa.

CAPITULO VI
DESCRIPCIÓN DEL PROYECTO

6.1 PROCESO DE ADMINISTRACIÓN DE SEGURIDAD

Ante la falta de un proceso de administración de seguridad que describa las actividades de planeación de la seguridad, detección, contención de incidentes, revisión de los planes de seguridad y de acuerdo a la falta de lecciones aprendidas en las empresas es necesario desarrollar formas de trabajo que nos permitan brindar seguridad informática adecuada para la toma de decisiones. Realizaremos un proceso que aplique para las cuatro dimensiones básicas de la seguridad en cualquier empresa: seguridad física, seguridad lógica, continuidad del negocio y control de fraudes, mediante la gestión de cada una de las áreas de seguridad correspondiente. Por consiguiente, se persigue prevenir, detectar, contener y corregir los incidentes de seguridad que se pudieran presentar.

Se considera de igual forma como problemática la falta de metodología y estrategia para la implantación de seguridad informática en las empresas, dada la falta de esquemas e importancia que se le da a la seguridad informática por la falta de percepción de costo-beneficio que no se clarifica hasta que se tiene un problema de seguridad en la empresa o institución.

La falta de identificación de dimensiones de la seguridad nos limita tener estrategias de cómo implantar y trabajar bajo esquemas de seguridad.

De ahí surge la necesidad de tener una plan de trabajo que nos determine qué actividades realizar para llevar a cabo el plan de seguridad por medio de lo expuesto en este trabajo.

Es recomendable conocer y entender el ISO 17799 que nos guía en los controles de seguridad internacionales ya que toda organización que haga uso de las tecnologías de información en necesario implantar buenas prácticas de seguridad puede generarnos huecos por no seguir algún proceso de implantación, por ejemplo, aumentando la posibilidad de riesgos en la información, así como, teniendo el riesgo de no facilitar el seguimiento en la forma de trabajo en la seguridad informática.

Por lo que es necesario que se lleve a cabo una identificación de las acciones a realizar para la administración de la seguridad y controles que deben ser considerados en una corporación para prevención de incidentes y fraudes.

Con este trabajo se pretende realizar un Planteamiento de la Seguridad Informática, en donde se describan las actividades de planeación, detección y contención de incidentes, así como la revisión de los planes de seguridad.

De igual forma, se plantea y esquematiza la forma de determinar las actividades de cada una de las personas que intervengan en la seguridad, así como describir las acciones a tomar. Según sea el problema, se tendrá que considerar cualquiera de los cuatro tipos de dimensiones que se trabajan frecuentemente.

Este proceso aplica para las cuatro dimensiones básicas de la seguridad propuesta:

- Seguridad física
- Seguridad lógica
- Continuidad del negocio
- Control de fraudes

Seguridad física. Es necesario prevenir el acceso de personas no autorizadas. Hay infinidad de información sobre cómo implantar seguridad física, pero no se lleva a cabo y mucho menos se sigue adecuadamente y lo importante es implantar e interactuar conjuntamente con las otras tres consideraciones básicas de seguridad.

Si cualquiera puede sentarse delante de una pc y comenzar a trabajar sin que nadie le diga nada, entonces se tiene un verdadero problema.

Importantísimo es el hecho de sensibilizar a los usuarios del sistema, sobre los riesgos que amenazan la seguridad física del equipo.

Seguridad lógica. La seguridad lógica se debe tener más en cuenta, ya que al estar conectados en red, la mayoría de ataques que podamos recibir irán hacia el software de servidores o aplicaciones. Para una buena seguridad lógica se deben tener en cuenta factores que involucren al usuario, el software y no del equipo de cómputo, como es el cambio periódico de password, asignación de firmas exclusivas por usuario, por mencionar algunas.

Continuidad del negocio (COB). Lo que se pretende con la continuidad es detectar las actividades imprescindibles para la organización para prevenir y

coordinar la contención y corrección de incidentes de seguridad que pongan en riesgo el negocio.[29]

Una clasificación del ciclo clásico para el proyecto de implantación de continuidad del negocio, COB, contempla lo siguiente:

- Entender e identificar las necesidades de la organización
- Planear un proyecto basado COB para la organización
- Analizar el riesgo y reducir el riesgo
- Analizar el impacto del riesgo
- Definir estrategia de continuidad
- Desarrollar planes de acción enfocados a COB
- Desarrollar e implantar procedimientos para un plan de mantenimiento COB
- Desarrollar e implantar un grupo de capacitación y un programa de pruebas en COB

Control de fraudes. Son las actividades para prevenir, detectar, contener y corregir incidentes de seguridad relacionados con el abuso o uso no autorizado de los servicios de una empresa o institución pública o particular.

Mediante la gestión de cada una de las áreas de seguridad correspondiente, se persigue prevenir, detectar, contener y corregir los incidentes de seguridad que se pudieran presentar. Determinando los factores que intervienen en la seguridad informática y seguridad de personal.

A continuación, algunos métodos de protección que pueden ser considerados.

- **VPN y VPDN.** Los VPN son redes privadas virtuales[30], VPDN (redes privadas virtuales dinámicas)[31]. Donde los datos se codifican y se envían a través de la conexión, protegiendo la información y el password.
- Creación de una DMZ, también conocida como zona desmilitarizada, nos permitirá tener una fiabilidad del acceso a nuestros sistemas de usuarios internos como externos.
- También puede ser implementado un sistema que utilice AAA (Autenticación, Autorización y Acceso)[32].

29 Hiles Andrew. Best Practices: World Class Business Continuity Management. Rothstein Associates, 2nd Edition, US, 2004
30 Tulloch, Mitch. Microsoft Encyclopedia of Security. Microsoft Press, US, 2003, Pág. 275
31 Tulloch , Mitch. Microsoft Encyclopedia of Security. Microsoft Press, US, 2003, Pág. 250

Como parte complementaria, se considera importante contemplar tres definiciones en la prevención de fraudes:

Autenticación. Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

Autorización. Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

Auditoría. Se refiere a la continua vigilancia de los servicios en producción. Entra en este rubro el hecho de mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por lo anterior, las políticas son la primera acción con que debe trabajar una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda y a normar la forma de trabajo dentro de la organización.

Con la ayuda de políticas, procedimientos y una cultura organizacional de seguridad en las empresas, la dirección general fomentará y apoyará la implantación de sistemas de riesgos, control y administración de seguridad, atacando la incertidumbre que se tiene de la seguridad.

32 Wylder, John. Strategic Information Security. Ed. Auerbach Publications, USA, 2004, Pág. 35

CAPÍTULO VII

MÉTODO

7.1 INTRODUCCIÓN

Es necesario realizar, en primera instancia, un análisis; posteriormente, determinar los riesgos que se tienen, de tal forma que la información obtenida justifique la inversión, la viabilidad del proyecto, la sugerencia de la solución, etc., para nuestra empresa.

En la Figura 7.1 se ejemplifica la forma en que se puede tener una relación con las distintas áreas y los permisos o perfiles que se pueden manejar; es un ejemplo de la forma en que la creación de cuentas que acceden a algún sistema con los perfiles. Desarrollar una matriz de riesgos ayudará a identificar el mayor riesgo que se tiene por la cantidad de accesos, perfiles y permisos que cada perfil cuenta para acceder a los sistemas de la empresa. Esto implica seguramente categorizar la información con la que se cuenta y determinar qué información es de alto, mediano y bajo riesgo, con la finalidad de determinar nuestras prioridades[33] en el momento de realizar alguna automatización o modificación en el sistema.

Matriz de Riesgos																
	Función	Confianza	Área 1	Eventual	Área 2	Área 3	Sistemas	Sindicalizados	Usuarios externos	Supervisor	Auditor	Cajero	Representante	Usuario de administración	Administrador	Totales	Riesgo (impacto por cantidad)
1	Consulta	X	X	X	X	X	X	X	X	X	X	X	X	X	X	14	14
2	Alta de representantes	X					X			X		X		X	X	6	12
3	Actualización de datos	X					X		X	X		X		X	X	7	21
4	Acreditar clientes	X	X	X	X	X		X					X			7	28
5	Modificar datos	X					X					X		X	X	5	25
6	Autorización	X			X	X	X	X	X			X		X	X	9	54
7	Revocar								X					X	X	3	21
8	Con privilegios						X	X	X				X	X	X	6	48
9	Mantenimiento						X					X		X	X	4	36
	Cantidad de funciones	6	2	2	3	3	7	4	5	3	1	6	3	8	8		
	Total de usuarios	217	1	89	14	5	7	548	10	2	3	8	20	2	2	**928**	
	Impacto (Perfil X Cantidad)	1302	2	178	42	15	49	2192	50	6	3	48	60	16	16		

Figura 7.1

Ahora bien, hay que diseñar un diagrama de flujo que nos ayude a identificar y guiar en la administración de la seguridad en nuestra empresa.

33 Gleim Irvin N. CIA review, Business Analysis and Information Technology. Gleim´s Publications Inc, Eleventh Edition, Florida, 2004 Part III, Pág. 443

Es necesario tomar decisiones teniendo en cuenta el tipo de incidente, la circunstancia y los niveles de riesgos que se identifiquen en la matriz antes mencionada. De igual forma, nos permitirá determinar si se cuenta con medidas de protección y metodología para su solución y pronto restablecimiento del servicio.
La matriz de la Figura 7.1 nos permitirá identificar las prioridades y riesgos en lo que debemos trabajar para mantener la integridad de la infraestructura de red, de igual forma pueden ser considerados y no necesariamente los siguientes puntos:

- Prevenir/descubrir el uso no autorizado
- Prevenir/descubrir el vandalismo intentado
- Prevenir/descubrir la malversación de información privada del cliente
- Asegurar contra la posibilidad de catástrofes
- La activación de planes de emergencia cuando los desastres ocurren

Mientras una organización proporcione un nivel alto de servicio a sus clientes, en contraste esto generalmente proporcionará el nivel de servicio cero a usuarios no autorizados. Principalmente implica la supervisión del uso de servicios para irregularidades y la actividad sospechosa, así como, la supervisión de información. Así también se requiere de la ejecución de planes de información que den a los usuarios y a los clientes una conciencia de los fraudes. La actividad es investigada para comprobar en la base de datos su integridad e inmediatamente ponerse en contacto con el cliente, la comunicación debe ser importante para el servicio que se puede dar en la prevención del fraude.

7.2 RESPONDER AL INCIDENTE

Evaluar lecciones aprendidas

Es indispensable informar a la corporación acciones y resultados obtenidos y definir los puntos en donde se tiene que realizar o crear políticas dentro de la empresa[34], esto es, la identificación de las debilidades y dependiendo de éstas, trabajar.

34 Schweitzer, Douglas. Incident Response: Computer Forensics Toolkit. John Wiley & Sons, USA 2003, Pág. 20

Para contemplar las respuestas a los incidentes identificados es necesario la creación de procedimientos de actividades, permitiendo identificar, la responsabilidad y vulnerabilidades en la operación, como puede ser en los casos de:

- Otorgar una cuenta
- Crear y dar de alta a un usuario
- Conectar una computadora a la red
- Actualizar el sistema operativo
- Instalar software localmente o vía red
- Actualizar software crítico
- Explorar sistemas de archivos
- Respaldar y restaurar información
- La forma de manejar un incidente de seguridad

A raíz de la evaluación de los casos que se pudieron haber presentado en una empresa por incidentes de seguridad, se recomienda transmitir la información o tratar de inferir en la forma de establecer la repercusión de vulnerabilidades que pueden impactar, por lo que hay que tener presente las medidas que asimilarán los empleados y los altos directivos, como son:

- Apoyar las medidas y soluciones
- Ser únicas las políticas
- Claras (explícitas)
- Concisas (breves)
- Estar bien estructuradas
- Servir de referencia
- Estar escritas
- Ser revisadas por abogados (si es necesario)
- Dadas a conocer a sus empleados
- Ser entendidas por los usuarios
- Ser firmadas por los usuarios
- Mantenerse actualizadas

De igual forma, se pretende llegar a estructurar las formas de respuesta y canalizar los incidentes de seguridad. Así mismo, determinar qué acciones seguir antes, durante y después del incidente.

Dado que la seguridad informática no es algo que se pueda implantar de un día para otro, es un proceso largo que implica mucha negociación con los directivos, ya que esta información debe ser completamente difundida y delimitada.

Las actividades relativas al plan de seguridad se deben llevar a cabo cada vez que se den cambios en los productos, la infraestructura o cuando la organización pudiera tener un impacto en el riesgo de fraude, por ejemplo. Las actividades para detectar incidentes de fraude serán continuas o por cada incidente, dependiendo del tipo de riesgo.

Se puede considerar la información mostrada en la Figura 7.1, para determinar el nivel de seguridad que se tiene y así definir las medidas a tomar.

A continuación, se muestra en la Tabla 7.1 la efectividad de las últimas políticas identificadas para seguridad informática[35].

Effectiveness of Policies & Procedures (percents Based on those whit policy or procedure in place)	Very or Extremely Effective	Somewhat Effective	Not Effective	Don´t know
Conduct regular security audits	51%	32%	8%	9%
Hired a Chief Security Officer (CSO) or Chief information Security Officer (CISO)	49%	23%	8%	19%
Periodic systems penetration testing	48%	30%	6%	16%
Monitor Internet connections	46%	35%	11%	8%
Periodic risk assessments	45%	36%	9%	10%
Use of an incident response team	44%	36%	7%	13%
Govemment security policy	43%	27%	12%	19%
Corporate security policy	42%	39%	11%	7%
Mandatory internal reporting of insider misuse(abuse)	40%	35%	16%	8%
Employee education & awareness programs	40%	43%	13%	4%
Employee/contractor background examination	40%	37%	10%	12%
Include security in contact negotiations with vendors(suppliers	39%	31%	11%	19%
Written "inappropriate use" policy	38%	40%	17%	4%
Regular security communication from management	37%	40%	17%	5%
New employee security trainiing	36%	44%	15%	6%
Require employees/ contractors to sing acceptable use policies	34%	41%	18%	6%
Use of "white hat" hackers	31%	32%	9%	28%
Employee monitoring	28%	45%	15%	12%
Storage & review of computer files	25%	38%	19%	18%
Storage & review of e-mail	24%	42%	18%	16%
Polygraph & examinations	20%	26%	19%	35%
Storage & review of voice mail	15%	30%	25%	30%
Record or review employee phone conversations	12%	27%	26%	36%

Tabla 7.1. Prácticas de seguridad informática

35 Survey. Secret Service & CERT. eCrime Watch Survey, Coordination Center, 2004, Pág. 10-12

Se observa en la Tabla 7.1 que la mejor práctica es la auditoría regular, ya que es una forma efectiva de identificar problemas y vulnerabilidades, por lo que hay que identificar los riesgos mostrado en la Figura 7.1 que se utilizó de ejemplo. Si bien no todas las compañías cuentan con una área de auditoría de sistemas, se puede ir trabajando para tener acciones de seguridad en nuestros equipos, desarrollos, sistemas, etc. De tal forma que se identifiquen vulnerabilidades o riesgos y se implementen medidas de seguridad acorde a las necesidades. Lo que nos permitirá contar con niveles de seguridad e identificación acceso a la información, evitándose gastos en contratación de especialistas ya que nos realizarán actividades que nosotros mismos podremos implantar reduciéndose gastos. Por ello es importante que las empresas inviertan en capacitación para sus administradores, evitándose contratar a externos en incidentes que pueden ser controlados de forma interna en la empresa.

CAPÍTULO VIII
PRODUCTO

Se sugiere desarrollar una metodología que brinde integridad de la infraestructura de red y de los servicios, previniendo, detectando y conteniendo riesgos como fraudes, accesos no autorizados, vandalismo, robo de información y desastres naturales.

Con este trabajo se crea una metodología que nos permita determinar incidentes de seguridad y las acciones a realizar. Así como identificar herramientas que ayuden con la administración y los roles que debe tener el administrador de seguridad. Generando un diagrama de flujo que nos ayude a determinar las acciones a tomar y se muestren los casos en los que se aplicarán las acciones a seguir. De igual forma determinar las políticas que debe seguir el personal para optimizar la ejecución de un proceso de seguridad, determinar cuáles son las políticas indispensables que se aplicarán en estructuras de red.

Se detallará en la forma de implantar seguridad informática considerando los recursos con los que se cuenta, de igual forma se trabajará en la forma en cómo tomar medidas correctivas y reactivas a incidentes de seguridad por cada uno de los roles que son definidos en la implantación de la seguridad.

En primer término es necesario identificar y definir las entradas y salidas existentes en nuestros sistemas, llevar a cabo la implantación de la administración de seguridad y proponer cómo se retroalimenta nuestro proceso de la información obtenido.

La principal idea es ser nosotros mismos auditores de nuestros sistemas, pero debemos considerar en dónde empezar y de ahí surgen estas ideas de identificar cuáles son nuestras entradas y salidas de información para determinar los pasos a seguir.

A continuación, se detalla el plan de trabajo con las consideraciones que se toman en cuenta para la solución, concluyendo con un resumen y un diagrama que facilitará el análisis.

8.1 OBJETIVO DEL PROCESO

Se determinará y trabajará en la integridad de la infraestructura de la empresa, según sea el rol del negocio, del personal, de los servicios, mediante la prevención,

detección y contención de riesgos de fraude, acceso no autorizado, vandalismo, robo y desastres naturales.

Se enlistan políticas que deben ser contempladas:

- Seguridad de información
- Continuidad del negocio
- Administración y logística
- Seguridad e higiene
- Reglas de actuación en el trabajo
- Contingencias en el desempeño del trabajo
- Seguridad corporativa en las instalaciones de la empresa
- Planes y procedimientos específicos de contingencia
- Herramientas tecnológicas de trabajo
- Redes y servicios de datos para uso corporativo
- Redes y servicios de voz para uso corporativo
- Rediseño de procesos, si es que es necesario
- Políticas de control de fraudes

Por lo que, se define como fraude al abuso o uso no autorizado de los servicios que la empresa presta a sus clientes.

Todo riesgo de fraude debe ser notificado inmediatamente al área de prevención de fraudes (control de fraudes), incluyendo todos los detalles que se soliciten, de acuerdo al riesgo específico.

Control de fraudes debe ser la única área autorizada para declarar un incidente de fraude.

Control de fraudes es la única área autorizada para determinar las acciones a tomar ante un posible incidente de fraude o ante un incidente de fraude ya declarado.

Las acciones solicitadas por control de fraudes ante un posible incidente de fraude, o ante uno ya declarado, no podrán ser contravenidas sin la autorización de control de fraudes o su línea directa de reporte.

Las acciones solicitadas por control de fraudes ante un riesgo de fraude deberán ser acatadas y ejecutadas por el área respectiva. En todo caso, ya sea que dichas medidas sean ejecutadas o que se presente una desviación, se deberá solicitar la aceptación del riesgo remanente al área respectiva y a la dirección de control del negocio, según sea el caso.

La aplicación de un crédito o reembolso a los clientes derivada de un incidente de fraude, será autorizada por el responsable del control de fraudes de acuerdo a las políticas que se definan en la empresa.

8.2 FRECUENCIA DEL PROCESO

Las actividades relativas al plan de seguridad se deben llevar a cabo cada vez que se den cambios en los productos, la infraestructura, sistemas o quien pudiera tener un impacto en el riesgo de fraude. Por lo que las actividades para detectar incidentes de fraude deben ser continuas o por cada incidente dependiendo del tipo de riesgo.

8.3 REGISTRO DERIVADO DEL PROCESO

Derivado de las actividades que fueron antes mencionadas es necesario realizar actividades, por lo que a continuación se proponen características y posibles tiempos de respuesta y la forma de dar seguimiento a incidentes, así como las acciones a seguir. En el Cuadro 8.1 se esquematizan las actividades, responsables y tiempos de respuesta.

Nombre del registro	Responsable de la custodia (rol)	Lugar de retención	Tiempo de retención	Disposición (caducidad)	Medio de protección
Correo electrónico con solicitud de intervención	Planeador de seguridad	Correo electrónico	1 año	Eliminación	Respaldo en servidor
Análisis de riesgo	Planeador de seguridad	Electrónico y/o impreso	COB: 1 año SL: 1 año CF: Permanente	Eliminación	Respaldo en servidor
Dictamen de riesgos	Planeador de seguridad	Electrónico y/o impreso	COB: 1 año SL: 1 año CF: Permanente	Eliminación	Respaldo en servidor
Plan de seguridad	Planeador de seguridad	Electrónico y/o impreso	Permanente según vigencia	Eliminación	Respaldo en servidor
Notificación de posible incidente de seguridad	Identificador de incidentes	Correo electrónico S / MIC	1 año	Eliminación	Respaldo en servidor
Declaratoria de incidente de seguridad	Ejecutor de medidas de seguridad	Correo electrónico	1 año	Eliminación	Respaldo en servidor
Declaratoria de cierre de incidente de seguridad	Ejecutor de medidas de seguridad	Correo electrónico	1 año	Eliminación	Respaldo en servidor
Minuta de lecciones aprendidas y registro de eventos	Planeador de seguridad	Correo electronico	COB: 1 año SL: 1 año CF: Permanente según vigencia	Eliminación	Respaldo en servidor

Cuadro 8.1. Descripción de actividades y responsabilidad

Derivado de la forma en cómo son canalizados los incidentes, se propone en el Diagrama 8.1 y 8.2, determinar e identificar la información, así como la responsabilidad que cada integrante del grupo de seguridad tendrá.

Las áreas de seguridad y operativas se describen a detalle. Posteriormente se planteará la implantación de un macroproceso general.

Diagrama del proceso

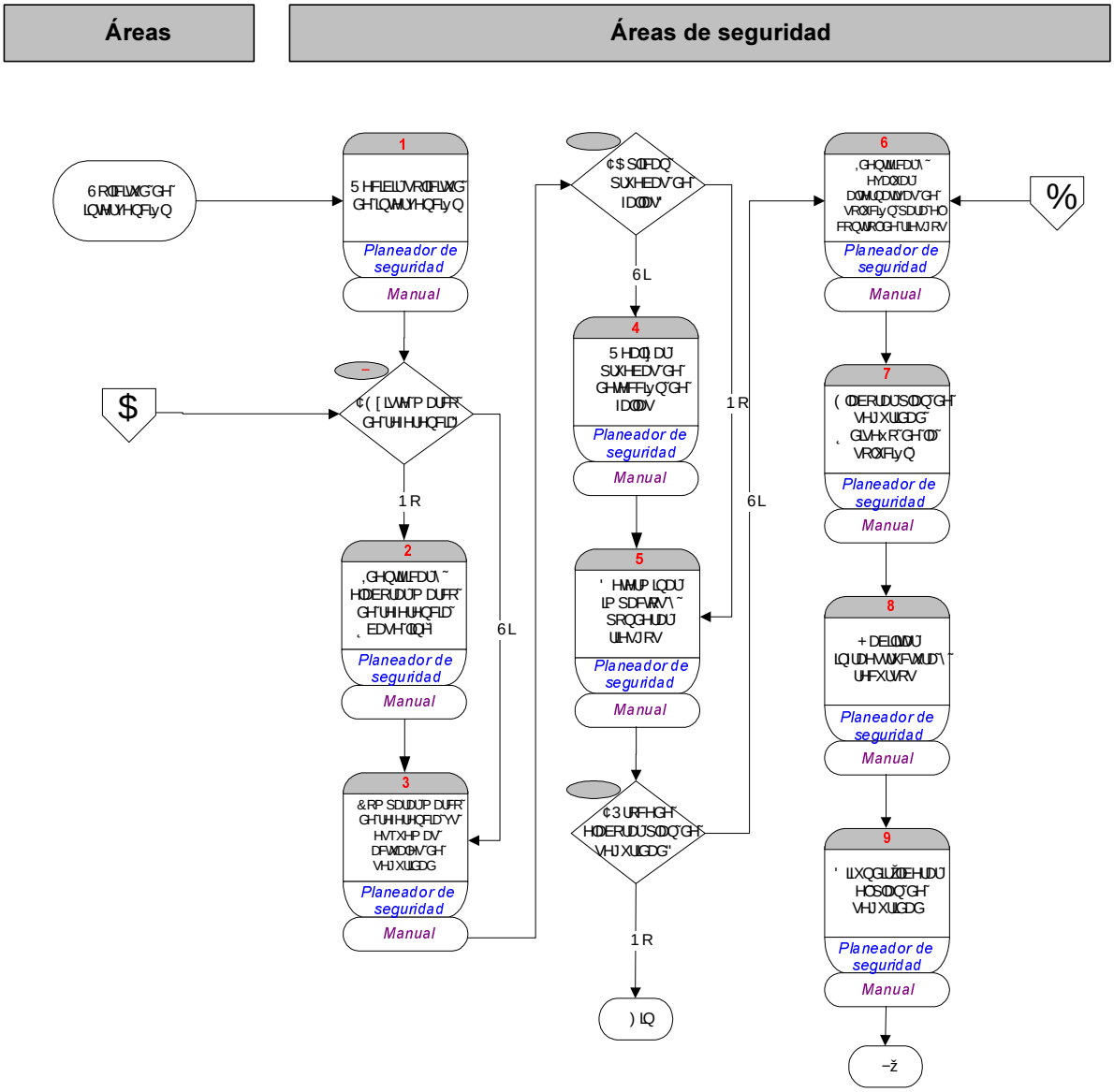


Diagrama 8.1

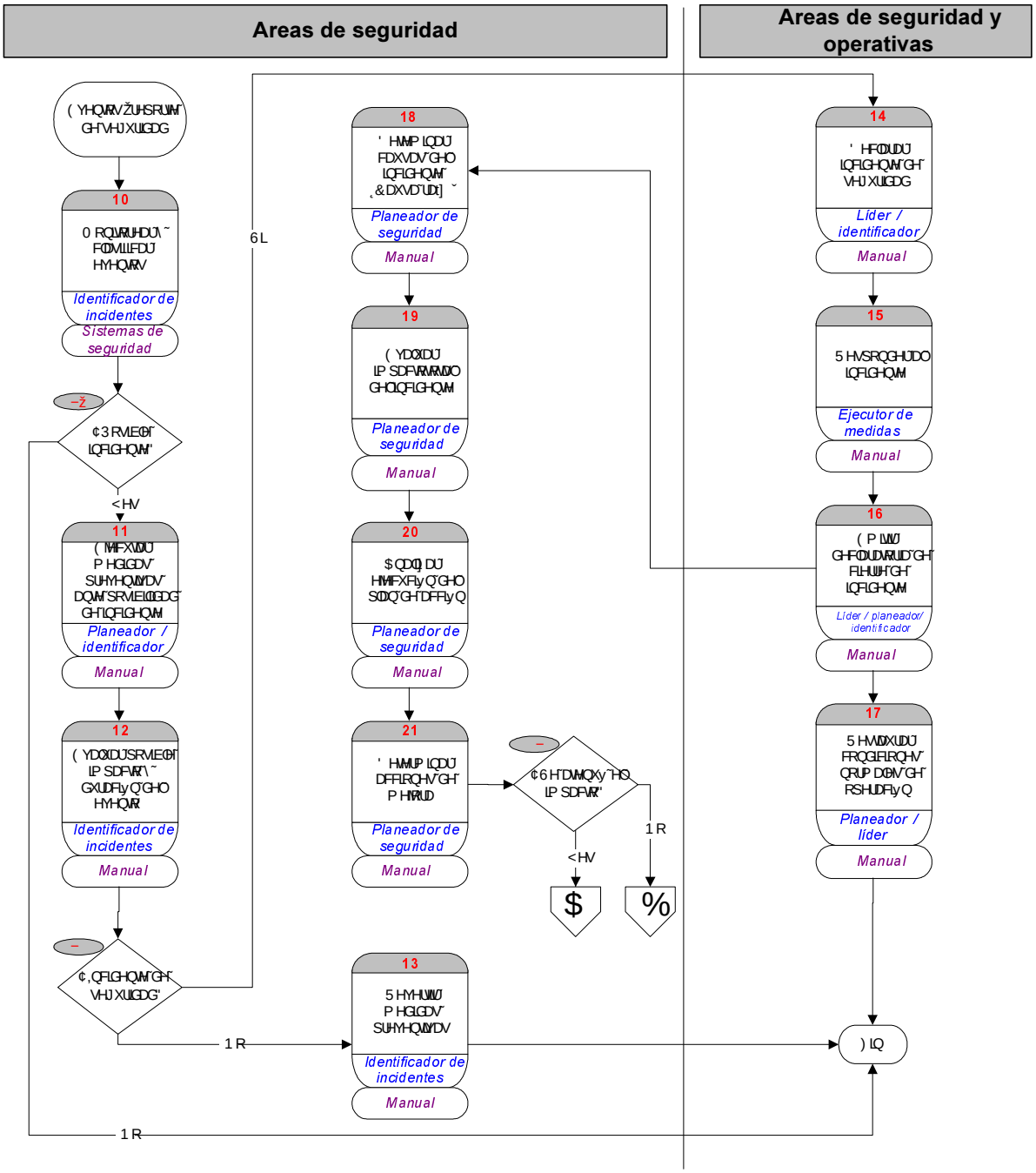

Areas de seguridad
Areas de seguridad y operativas
10
Identificador de incidentes
Sistemas de seguridad
11
Planeador / identificador
Manual
12
Identificador de incidentes
Manual
13
Identificador de incidentes
Manual
18
Planeador de seguridad
Manual
19
Planeador de seguridad
Manual
20
Planeador de seguridad
Manual
21
Planeador de seguridad
Manual
14
Líder / identificador
Manual
15
Ejecutor de medidas
Manual
16
Líder / planeador/ identificador
Manual
17
Planeador / lider
Manual
6L
1R
1R
<HV
1R
<HV
$
%

Diagrama 8.2

8.4 DESCRIPCIÓN DETALLADA DEL PROCESO

A continuación, se detallan las actividades y tareas que se muestran en el Diagrama 8.1 y 8.2 con la finalidad de clarificar las acciones a desarrollar.

	TAREA	DESCRIPCIÓN	APLICACIONES
1	Recibir solicitud de intervención	El planeador de seguridad recibe la solicitud para que el área respectiva de seguridad intervenga para mantener la integridad de la infraestructura o de los servicios, ante un posible riesgo generado por un cambio en la operación o en la infraestructura, o por la implantación de una política, o de acuerdo a los esquemas de revisión periódicos. El planeador de seguridad revisará si existe un marco de referencia para el posible riesgo. Si existe un marco de referencia, se procederá con la actividad "Comparar marco de referencia vs. esquemas actuales de seguridad" (actividad 3) Si no existe marco de referencia para el riesgo, se procederá con la actividad "Identificar y elaborar marco de referencia" (actividad 2).	Manual (telefónico, mail), E-mail, FMS
2	Identificar y elaborar marco de referencia *(base line)*	El planeador de seguridad realiza las siguientes actividades: • Investigará políticas corporativas • Investigará normatividad • Investigará mejores prácticas • Estudiará tendencias históricas • Investigará reglas de negocio • Estudiará lecciones aprendidas Una vez que se terminan las actividades anteriores, el planeador de seguridad elabora un documento que incluye un resumen de lo investigado (*base line)*.	Manual

	TAREA	DESCRIPCIÓN	APLICACIONES
3	Comparar marco de referencia vs esquemas actuales de seguridad	El planeador de seguridad compara los esquemas de seguridad actuales contra el marco de referencia y documenta los resultados de la comparación. El planeador de seguridad determina la necesidad de realizar pruebas de detección de fallas y / o vulnerabilidades. Si la decisión es realizar pruebas, continuar con la realización de pruebas de detección de fallas (actividad 4). Si la decisión es no realizar pruebas, continuar con determinar impactos y ponderar riesgos (actividad 5).	Manual
4	Realizar pruebas de detección de fallas	El planeador de seguridad realiza o solicita las pruebas pertinentes para detectar las vulnerabilidades en el esquema de seguridad actual.	Manual,FMS, Nessus / Nmap, ISS
5	Determinar impactos y ponderar riesgos	El planeador de seguridad determina y pondera impactos tangibles e intangibles de los riesgos. El planeador de seguridad consolida los resultados de: • Comparar el marco de referencia contra el esquema actual de seguridad, • Las pruebas para la detección de vulnerabilidades, • La ponderación de impactos El planeador de seguridad genera un documento detallando el riesgo, las vulnerabilidades y el impacto al negocio. Si de acuerdo al dictamen de riesgos no aplica la elaboración de un plan de seguridad, se procederá a informar al área respectiva que no procede elaborar un plan de seguridad y ahí se terminan las actividades. Si de acuerdo al dictamen de riesgos sí aplica la elaboración de un plan de seguridad, se procede a identificar y evaluar alternativas de solución para el control de riesgos (actividad 6)	Manual

	TAREA	DESCRIPCIÓN	APLICACIONES
6	Identificar y evaluar alternativas de solución para el control de riesgos	El planeador de seguridad, con base en el documento detallado del riesgo, identifica las alternativas de acuerdo con los siguientes criterios: • Legales • Tecnológicas • Organizacionales Cuando se tienen identificadas las alternativas, el planeador de seguridad las evalúa tomando en cuenta los siguientes criterios: • Implantación • Eficiencia y eficacia • Mejores prácticas y tendencias históricas • Costo-beneficio • Implicaciones (legales, tecnológicas, organizaciones, etc.) • De acuerdo con los resultados obtenidos de la evaluación, el planeador de seguridad selecciona la alternativa de solución	Manual
7	Elaborar plan de seguridad (diseño de la solución)	El planeador de seguridad elabora el plan de seguridad, el cual incluye los siguientes rubros: • Definición de procedimientos • Definición de estrategias de detección • Definición de estrategia de prevención • Definición de estrategias de contención • Definición de estrategias de recuperación • Definición de estrategias de medición Cuando ya se tiene el plan de seguridad el planeador de seguridad realiza: • Definición de requerimientos para la implantación de la solución (infraestructura, recursos, servicios, etc.) • Definición de dependencias para la implantación de la solución	Manual

	TAREA	DESCRIPCIÓN	APLICACIONES
8	Habilitar infraestructura y recursos	El planeador de seguridad coordina la habilitación de la infraestructura acorde con las siguientes tareas: • Instalar barreras de protección y / o perimetrales. • Instalar equipos, sistemas y servicios. • Requerir proyecto de infraestructura de red. • Habilitar recursos humanos necesarios. • Correr pruebas y realizar ajustes. Cuando las pruebas son satisfactorias, el planeador de seguridad entregará a personal que trabaje con los sistemas de producción.	COB: Manual CF: Manual, FMS SL: Plataforma de Firewalls / Proxeo Plataforma de IDS's Plataforma de autenticación. Plataforma de vulnerability scanning SF: Ccure 800
9	Difundir / liberar el plan de seguridad	El planeador de seguridad realiza la capacitación del plan de seguridad, coordina las pruebas para certificar la capacitación y el plan, cuando haya desviaciones realiza las correcciones correspondientes. Cuando no existan desviaciones, el planeador de seguridad difunde y libera el plan de seguridad.	Manual
10	Monitorear y clasificar eventos	El identificador de incidentes monitorea todos los eventos relacionados con seguridad y / o recibe los reportes de seguridad correspondientes. El identificador de incidentes reconoce los eventos y reportes de seguridad que pudieran ser incidentes de seguridad de acuerdo a los criterios definidos en el plan de seguridad. El monitoreo tiene la función de detectar incidentes en las dimensiones lógica, física, fraudes y continuidad del negocio. Nota: El monitoreo incluye reportes de seguridad/alerta temprana (warnings) provenientes de entidades internas, así como externas. Si se reconoce un posible incidente de seguridad se procede a ejecutar las medidas de prevención ante posibilidad de incidente (actividad 11). Si no se reconoce un posible incidente de seguridad, se registra el evento según corresponda, finalizando las actividades.	COB: Plataformas de gestión de transmisión, datos, voz y seguridad, Outlook. CF: Manual, Base de Datos de casos, FMS SL: Plataforma de detección de intrusos y sistemas externo de alertas tempranas SF: Ccure800, en Outlook

	TAREA	DESCRIPCIÓN	APLICACIONES
11	Ejecutar medidas preventivas ante posibilidad de incidentes	El planeador de seguridad, cuando identifica desviaciones, actúa de acuerdo con las acciones definidas en el plan de seguridad correspondiente.	COB: Manual CF: Manual, FMS, Plataformas de servicios SL: Manual SF: Manual
12	Evaluar posible impacto y duración del evento	El identificador de incidentes recopilará todos los elementos para evaluar el impacto y duración del evento, recurriendo para ello a las áreas y fuentes de información que sean necesarias conforme al plan de seguridad. Si se determina que el evento es un incidente de seguridad, se procederá a declarar el incidente de seguridad (actividad 14). Si se determina que el evento no es un incidente de seguridad, se registra el evento según corresponda, y se procede a revertir medidas preventivas (actividad 13).	Manual
13	Revertir medidas preventivas	El identificador de incidentes revierte las acciones preventivas que se hubieran tomado.	Manual
14	Declarar incidente de seguridad	El líder del plan de seguridad/identificador de incidentes, notifica a los afectados, por los medios respectivos y formaliza la declaratoria de incidente de seguridad. Al formalizarse la declaratoria de incidente de seguridad, se debe solicitar la ejecución de las medidas de respuesta al incidente conforme al plan de seguridad.	COB: Manual CF: E-mail, Base de datos de casos, FMS SL: Manual, Sistema de detección de intrusos SF:Outlook, Sistemas de detección
15	Responder al incidente	El ejecutor de medidas actúa de acuerdo con el plan de seguridad. Sus funciones están basadas en los siguientes rubros: • Ejecutar medidas de contención • Ejecutar medidas de corrección • Registrar detalles del seguimiento al incidente	Manual

	TAREA	DESCRIPCIÓN	APLICACIONES
16	Emitir declaratoria de cierre de incidente	El líder del plan de seguridad, en conjunto con el planeador de seguridad y el identificador de incidentes, recopilan todos los elementos para emitir la declaratoria de cierre de Incidente, de acuerdo a los resultados de las medidas de contención y corrección, ejecutadas por las áreas respectivas y con base en las fuentes de información, conforme al plan de seguridad. Una vez que se emite la declaratoria del cierre del incidente de seguridad se debe notificar a las áreas respectivas para que regresen a sus funciones normales y se procede a identificar características del incidente (actividad 18) para comenzar con las actividades de "Lecciones Aprendidas".	Manual, Outlook
17	Restaurar condiciones normales de operación	El líder del plan de seguridad/planeador de seguridad coordinará las acciones de regreso a condiciones normales de operación.	Manual
18	Determinar causas del incidente (causa raíz)	El planeador de seguridad recopila todos los elementos necesarios para determinar la causa raíz del incidente, recurriendo para ello a las áreas especializadas y / o fuentes autorizadas.	Manual
19	Evaluar impacto total del incidente	El planeador de seguridad realiza las siguientes tareas: • Inventario de daños • Evalúa impactos legales • Evalúa impactos económicos • Evalúa impactos organizacionales Para esta actividad se obtiene la información de los grupos participantes y / o áreas afectadas.	Plataformas de gestion de transmisión, datos, voz y seguridad, Outlook Manual, MIC, FMS Manual SF: Manual
20	Analizar ejecución del plan de acción	El planeador de seguridad analiza la eficiencia y eficacia del plan con base en los resultados de la aplicación del plan, identificando las brechas y / o áreas de oportunidad.	Manual

	TAREA	DESCRIPCIÓN	APLICACIONES
21	Determinar acciones de mejora	El planeador de seguridad propone las acciones encaminadas a mejorar el plan de seguridad o a la creación del mismo en caso de que el incidente no estuviera identificado se considerará algún plan de seguridad o acción a seguir. El planeador de seguridad debe mantener un registro histórico de los incidentes de seguridad que se hayan presentado. En caso de que el incidente ya esté contemplado en un plan de seguridad, se procede a identificar y evaluar alternativas de solución para el control de riesgo (actividad 6). En caso de que el incidente no esté contemplado en un plan de seguridad, se procede a investigar si existe un marco de referencia que lo contenga (actividad 1) y continuar con las actividades subsecuentes.	Manual

A continuación, se plantean las acciones que se deben contemplar como entradas y salidas del procedimiento a seguir en la seguridad informática.

8.5 TABLA DE ENTRADAS / SALIDAS DEL PROCESO

	Entradas			Salidas		
	Descripción	**Origen**	**Soporte**	**Descripción**	**Destino**	**Soporte**
1	Solicitud de intervención para mantener la seguridad	Áreas de la empresa	Documento electrónico o impreso	Si existe un marco de referencia, se procederá con la actividad "Comparar marco de referencia vs esquemas actuales de seguridad" (3). Si no existe marco de referencia para el riesgo se procederá con la actividad "identificar y elaborar marco de referencia" (2)	Planeador de seguridad	Manual
2	Políticas corporativas, normatividad, mejores prácticas, tendencias historicas, reglas de negocio, lecciones aprendidas	Áreas de seguridad fuentes autorizadas	Documento electrónico o impreso	Marco de referencia	Comparar marco de referencia vs esquemas actuales de seguridad (actividad 3)	Documento impreso y/o electrónico
3	Marco de referencia para solicitud de intervención	Identificar y elaborar Marco de referencia (actividad 2) y/o información proveniente de la base de conocimiento del área de seguridad Recepción de solicitud de intervención (actividad 1)	Documento impreso y/o electrónico	Descripción de brechas entre el marco de referencia y el esquema actual de seguridad y/o solicitud de realización de pruebas de fallas en caso de ser necesario.	Determinar impactos y ponderar riesgos (actividad 5) y/o realizar pruebas de detección de fallas (actividad 4)	Documento impreso y/o electrónico

	Entradas			Salidas		
	Descripción	**Origen**	**Soporte**	**Descripción**	**Destino**	**Soporte**
4	Solicitud de realización de pruebas de fallas. Descripción de brechas entre el marco de referencia y el esquema actual de seguridad y/o solicitud de realización de pruebas de fallas en caso de ser necesario.	Comparar marco de referencia vs esquemas actuales de seguridad. (actividad 3)	Documento impreso y/o electrónico	Resultados de las pruebas de fallas y brechas entre el marco de referencia y el esquema actual de seguridad	Determinar impactos y ponderar riesgos (actividad 5)	Documento impreso y/o electrónico
5	Descripción de brechas entre el marco de referencia y el esquema actual de seguridad Resultados de las pruebas de fallas	Comparar marco de referencia vs esquemas actuales de seguridad (actividad 3) y/o realizar pruebas de detección de fallas (actividad 3)	Documento impreso y/o electrónico	Descripción y ponderación de los impactos de los riesgos identificados (dictamen de riesgos)	Si aplica elaborar un plan de seguridad, se envía a Identificar y evaluar alternativas de solución (actividad 6). Si no aplica, se informa al área respectiva el plan, finalizando las actividades	Documento impreso y/o electrónico
6	Dictamen de riesgos	Determinar impactos y ponderar riesgos (actividad 5)	Documento impreso y/o electrónico	Propuesta de solución	Elaborar plan de seguridad (diseño de la solución) (actividad 7)	Documento impreso y/o electrónico
7	Propuesta de solución	Identificar y evaluar alternativas de solución para el control de riesgos (actividad 6)	Documento impreso y/o electrónico	Plan de seguridad requerimientos para la implantación del plan de seguridad	Habilitar infraestructura y recursos (actividad 8)	Documento impreso y/o electrónico

	Entradas			Salidas		
	Descripción	**Origen**	**Soporte**	**Descripción**	**Destino**	**Soporte**
8	Plan de seguridad seguridad para la implantación del plan de seguirdad requerimientos para la implantación del plan de seguridad	Elaborar plan de seguirdad, diseño de la solución (actividad 7)	Documento impreso y/o electrónico	Infraestructura y recursos habilitados	Difundir/liberar el plan de seguridad	Documento impreso y/o electrónico Notificaciones de las áreas respectivas
9	Infraestructura y recursos habilitados	Habilitar infraestructura y recursos (actividad 8)	Documento impreso y/o electrónico Notificaciones de las áreas respectivas	Difusión y liberación del plan de seguridad, documentos de referencia	Áreas correspondientes	Documento impreso y/o electrónico
10	Eventos / reportes de seguridad	Cualquier actividad de la empresa	Documentos y registros impresos y/o electrónicos	Si existe la posibilidad de un incidente de seguridad, se envía la solicitud de ejecución de medidas de control Si no existe posibilidad de un incidente de seguridad, se registra el evento y se finalizan las actividades	Si existe la posibilidad de un incidente de seguridad, se envía la solicitud a la actividad 11 Si no existe posibilidad de un incidente de seguridad, el registro se envía a la base de datos del área de seguridad respectiva	Documento impreso y/o electrónico
11	Solicitud de ejecución de medidas preventivas	Monitorear y clasificar eventos (actividad 10)	Documento impreso y/o electrónico	Resultado de las medidas de prevención	Evaluar posible impacto y duración del evento (actividad 12)	Documento impreso y/o electrónico

	Entradas			Salidas		
	Descripción	**Origen**	**Soporte**	**Descripción**	**Destino**	**Soporte**
12	Resultado de las medidas de prevención	Ejecutar medidas preventivas ante posibilidad de incidente	Documento impreso y/o electrónico	Solicitud de revertir medidas preventivas en el caso de que se determine que no es un incidente de seguridad (actividad 13). Detalles del impacto y duración del evento, en caso de que se determine que el evento es un incidente de seguridad (actividad 14)	Revertir medidas preventivas (actividad 13) o declarar incidente de seguridad (actividad 14)	Documento impreso y/o electrónico
13	Solicitud de revertir medidas preventivas en el caso de que se determine que no es un incidente de seguridad.	Evaluar posible impacto y duración del evento (actividad 12)	Documento impreso y/o electrónico	Medidas preventivas revertidas	FIN	Documento impreso y/o electrónico
14	Detalles del impacto y duración del evento, en caso de que se determine que el evento es un incidente de seguridad.	Evaluar posible impacto y duración del evento (actividad 12)	Documento impreso y/o electrónico	Solicitud de ejecución de las medidas de respuesta al incidente Información sobre el incidente	Responder al incidente (actividad 15)	Documento impreso y/o electrónico
15	Solicitud de ejecución de las medidas de respuesta al incidente. Información sobre el incidente.	Declarar incidente de seguridad (actividad 14)	Documento impreso y/o electrónico	Detalle del seguimiento al incidente de seguridad y resultados de la ejecución de medidas de contención y corrección	Emitir declaratoria de cierre de incidente (actividad 16)	Documento impreso y/o electrónico

	Entradas			Salidas		
	Descripción	**Origen**	**Soporte**	**Descripción**	**Destino**	**Soporte**
16	Detalle del seguimiento al incidente de seguridad y resultados de la ejecución de medidas de contención y corrección	Responder al incidente. (actividad 15)	Documento impreso y/o electrónico	Declaratoria de cierre de incidente y solicitud de regreso a las condiciones normales de operación	Restaurar condiciones normales de operación (actividad 17)	Documento impreso y/o electrónico
17	Declaratoria de cierre de incidente y solicitud de regreso a las condiciones normales de operación	Emitir declaratoria de cierre de incidente (actividad 16)	Documento impreso y/o electrónico	Condiciones normales de operación reestablecidas	Determinar causas del incidente, causa raíz (actividad 18)	Documento impreso y/o electrónico
18	Detalle del seguimiento al incidente de seguridad (Inicio a fin)	Restaurar condiciones normales de operación (actidad 17)	Documento impreso y/o electrónico	Causa raíz identificada	Evaluar impacto total del incidente (actividad 19)	Documento impreso y/o electrónico
19	Información sobre los impactos particulares de parte de los grupos participantes en la atención al incidente de seguridad y/o áreas afectadas	Determinar causas del inci- dente, causa raíz (actividad 18)	Documento impreso y/o electrónico	Impacto total del incidente	Analizar ejecución del plan de seguridad (actividad 20)	Documento impreso y/o electrónico
20	Detalle del seguimiento al incidente de seguridad (inicio a fin)	Evaluar impacto total del incidente (actividad 19)	Documento impreso y/o electrónico	Eficiencia y eficacia en la ejecución del plan, y brechas y áreas de oportunidad	Determinar acciones de mejora (actividad 21)	Documento impreso y/o electrónico

	Entradas			Salidas		
	Descripción	**Origen**	**Soporte**	**Descripción**	**Destino**	**Soporte**
21	Eficiencia y eficacia en la ejecución del plan y brechas y áreas de oportunidad	Analizar ejecución de plan de seguridad (actividad 20)	Documento impreso y/o electrónico	Acciones propuestas para la creación / mejora del plan de seguridad	En caso de que el incidente ya esté contemplado en un plan de seguridad, identificar y evaluar alternativas de solución para el control del riesgo (actividad 6) En caso contrario, se investigará si existe un marco de referencia (actividad 1)	Documento impreso y/o electrónico

La necesidad de acción y de medidas que deban ser consideradas para la intervención en casos de incidentes de seguridad, da como consecuencia detallar las circunstancias en que podremos determinar el incidente. Con la finalidad de crear un marco de referencia que permita ligar las políticas de seguridad, las mejores prácticas, las tendencias históricas, las reglas de negocio y las lecciones aprendidas que deben ser consideradas en la empresa y por el responsable de la seguridad informática, nos lleva a especificar y detallar cada una de las actividades del diagrama 8.1 y 8.2. En el punto 8.5 se describen las entradas y salidas que se identifican en cualquier situación, el origen y el soporte que en caso de incidente de seguridad se debe tomar en cuenta, pretendiendo ser la guía importante a analizar. De esta forma, las acciones pueden ser consideradas según sea el caso y las características que determine el negocio de la empresa.

Por lo descrito anteriormente, es necesario representar dichas actividades en una forma esquemática que nos facilite la identificación de roles y actividades que deben ser realizadas.

En las siguientes páginas se mostrará la forma esquemática de lo propuesto y descrito en los diagramas 8.1 y 8.2 detallando la cadena de administración de seguridad.

Figura 8.1

Se considerará, en primera instancia, la forma en que identificaremos la información para la administración que se llevará a cabo, por consiguiente, se obtendrá en la salida o resultado, el alimentador de otras actividades de seguridad como se muestra en el Figura 8.1.

Es importante considerar en nuestro análisis de seguridad, la información con que se cuenta, como puede ser alarmas e indicadores en nuestros sistemas, el monitoreo, generación de reportes, etc.

La metodología que se sugiere desarrollar se basará en un diagrama que permita a empresas determinar los casos y las actividades que deban realizarse en incidentes de seguridad y en la implantación de la seguridad corporativa.

En la siguiente página, se resume el planeamiento de seguridad.

Secuencia de actividades: Administración de la seguridad

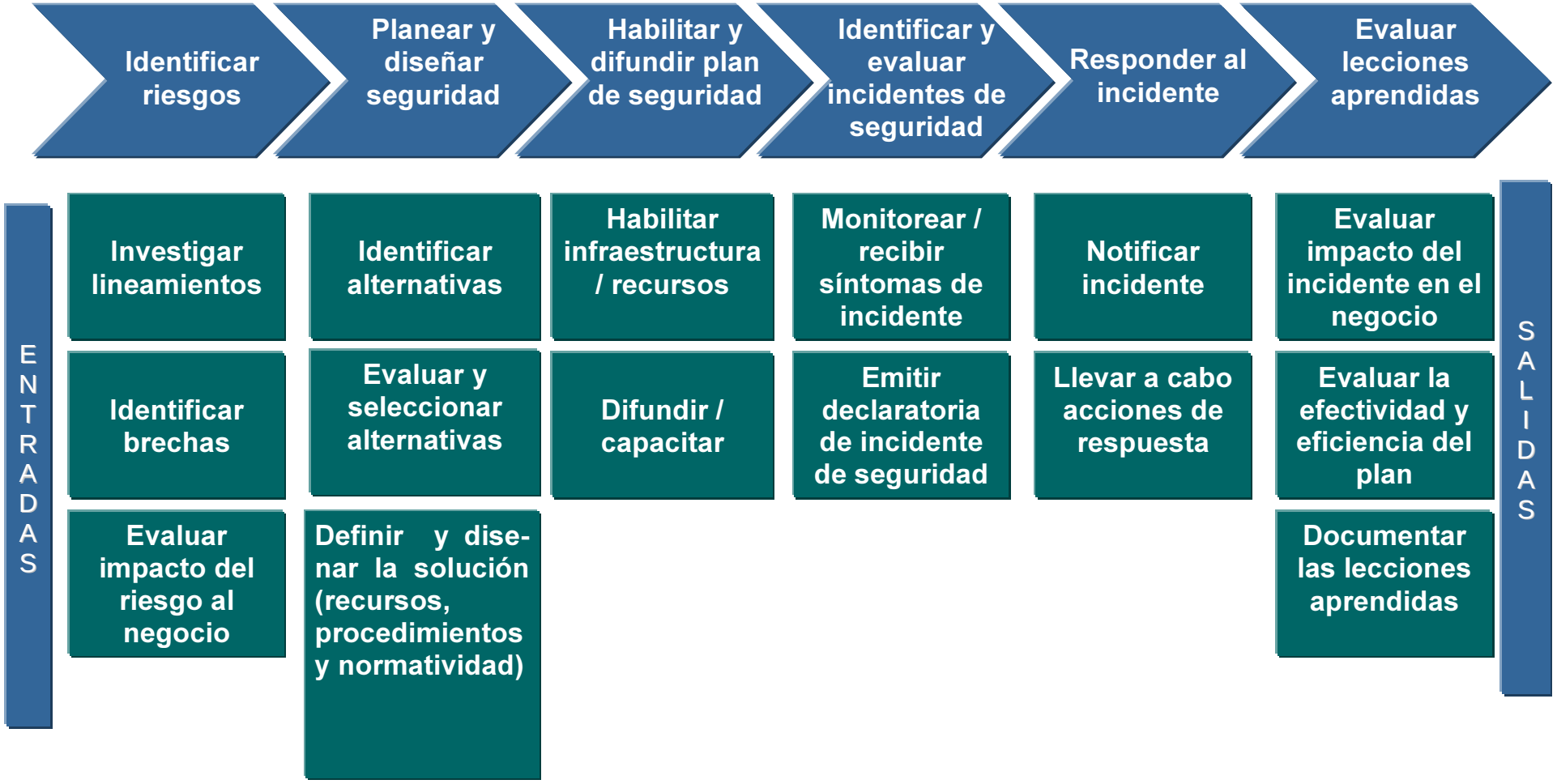


Diagrama 8.3

En el Diagrama 8.3, se determinan las actividades y los procesos, así como el esquema general que es considerado en algún incidente de seguridad, como son la identificación del riesgo, el planear y diseñar seguridad, habilitación y difusión del plan de seguridad, identificar y evaluar incidentes, responder al incidente y evaluación de lecciones aprendidas.

Lo anterior, nos esquematiza las áreas y los puntos que debemos trabajar a detalle y en lo que nos enfocaremos en caso de algún incidente.

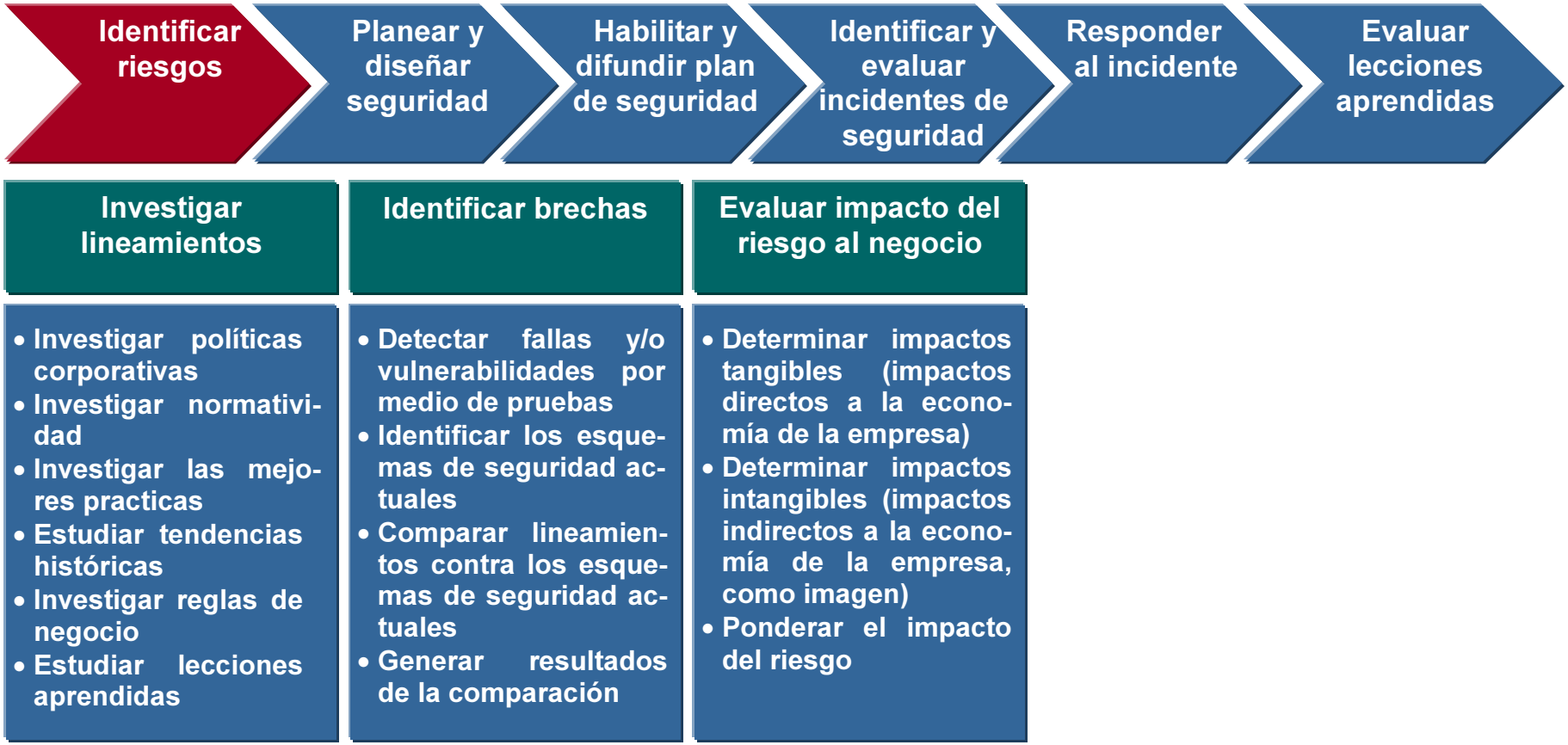
En primera instancia, se trabajará en identificar los riesgos. Resulta evidente que al contar con sistemas de información y con áreas de operación no se tenga el concepto de riesgos presente, ya que al cuestionar a cualquier persona sobre sus actividades, la respuesta será que:

- Todo se hace correctamente
- No se tiene ningún riesgo
- Todo lo que hago tiene un alto impacto en la operación

Dado que se pueden tener problemas para determinar el grado de riesgo (alto, medio o bajo), la primera actividad consiste en identificar las actividades que se realizan, el personal que accede a la información, cantidad de firmas, permisos, etc., como se muestra en la Figura 7.1. Lo que nos llevará a tres actividades posteriores: identificar e investigar los lineamientos de la empresa, identificar brechas y evaluar el impacto del riesgo al negocio.

A continuación, se describirá lo visto en el Diagrama 8.3 detallando las actividades que se deben llevar a cabo, según la etapa en que se encuentre el incidente de seguridad.

Secuencia de actividades: Administración de la seguridad



Secuencia de actividades: Administración de la seguridad

Identificar alternativas de minimización de riesgo

- Identificar alternativas legales
- Identificar alternativas tecnológicas
- Identificar alternativas organizacionales
- Identificar alternativas normativas

Evaluar y seleccionar alternativas

- Evaluar tiempo de implantación
- Evaluar y predecir la eficiencia y eficacia de la solución propuesta, de acuerdo a los lineamientos (tendencias históricas, Best Practices)
- Evaluar costos de implantación y operación
- Evaluar implicaciones (legales, tecnológicas, organizacionales, etc.)

Definir y diseñar la solución

- Definir requerimientos para la implantación de la solución (infraestructura, recursos, servicios, etc.)
- Definir dependencias para la implantación de la solución
- Definir procedimientos
- Definir estrategia de prevención
- Definir estrategias de detección
- Definir estrategias de contención

- Definir estrategias de recuperación
- Definir estrategias de medición
- Elaborar plan de seguridad

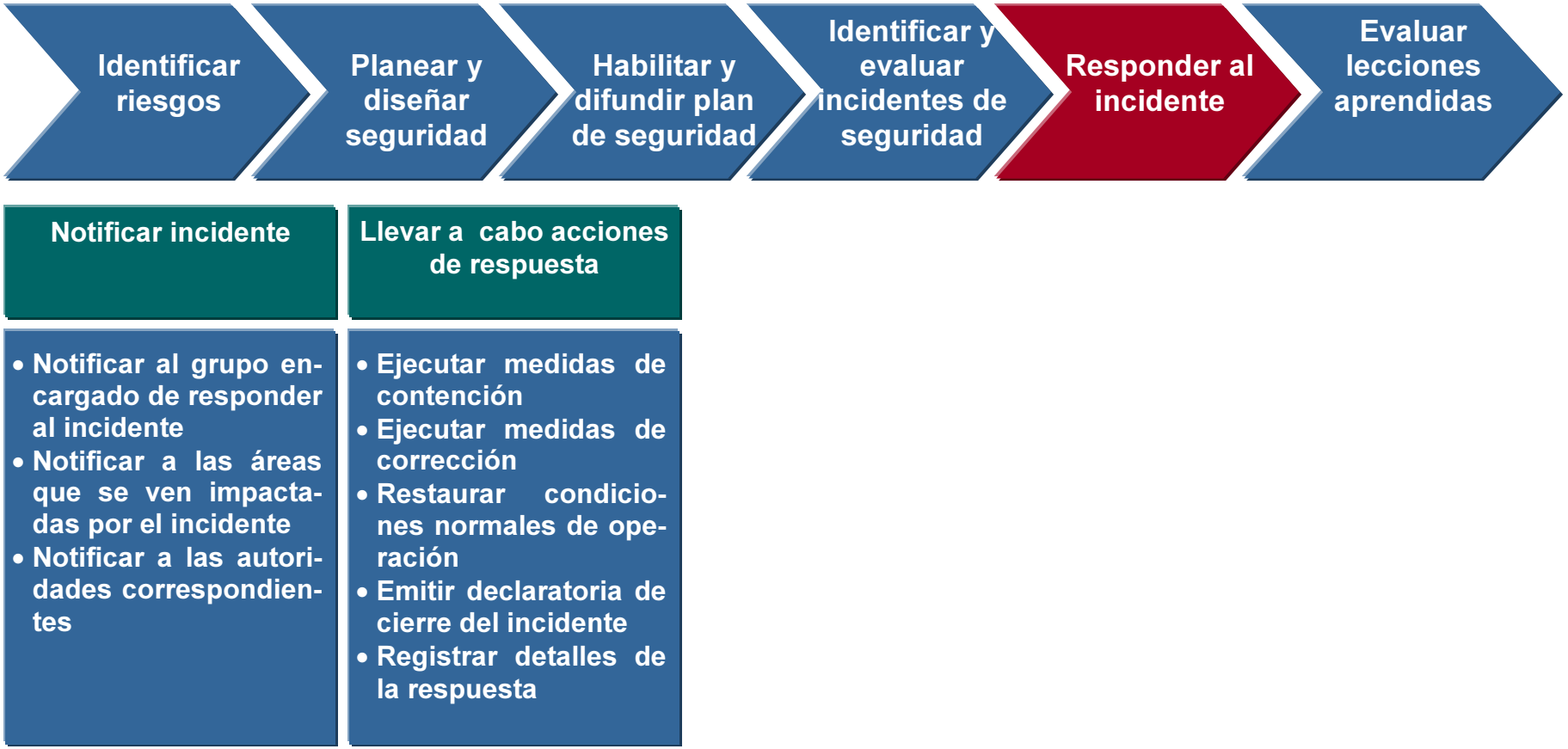
Secuencia de actividades: Administración de la seguridad

Habilitar infraestructura / recursos	Difundir / capacitar el plan de seguridad
• Instalar barreras de protección y / o perimetrales • Instalar equipos, sistemas y servicios • Requerir proyecto de infraestructura de red • Habilitar recursos humanos necesarios • Correr pruebas y hacer ajustes	• Capacitar áreas involucradas sobre la estrategia de seguridad • Ejercitar / ajustar el plan (simular las condiciones de un incidente) • Liberar / difundir plan de seguridad a la organización

Secuencia de actividades: Administración de la seguridad

Monitorear/ recibir síntomas de incidente	Emitir declaratoria de incidente de seguridad
• Monitorear para detectar incidentes (lógicos, físicos, fraudes y continuidad del negocio) • Recibir reporte de eventos relacionados a la seguridad • Recibir advertencia por entidades externas • Registrar eventos predictibles • Ejecutar medidas de prevención ante la posibilidad de un incidente y registrar detalle de dichas medidas	• Analizar síntomas de incidente • Evaluar impactos al negocio • Determinar la duración del evento • Generar declaración de incidente • Registrar detalles del incidente

Secuencia de actividades: Administración de la seguridad



Secuencia de actividades: Administración de la seguridad

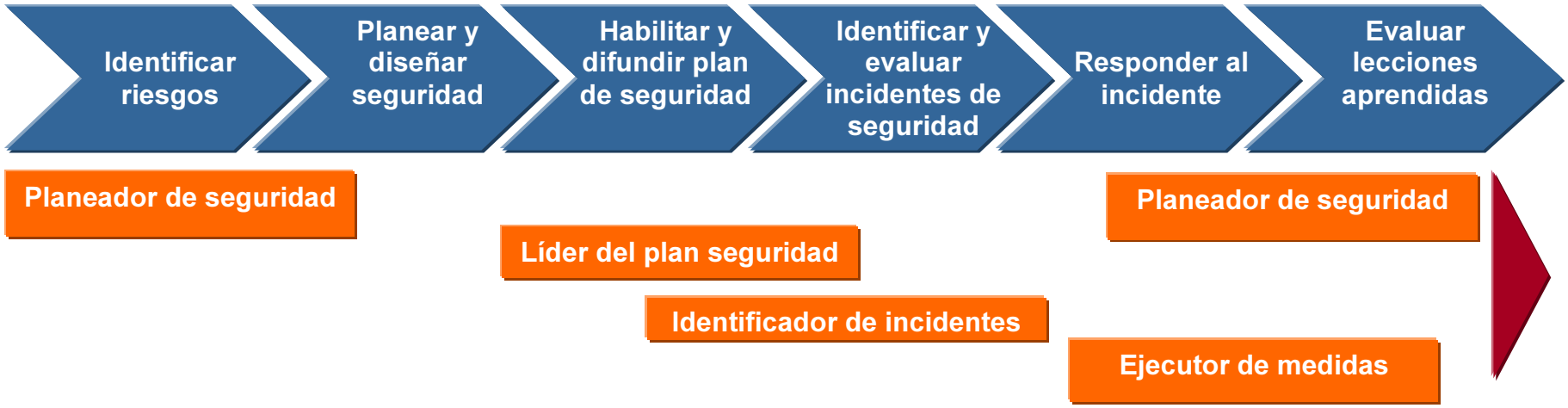
Evaluar impacto del incidente en el negocio

- Determinar causas del incidente (causa raíz)
- Realizar inventario de daños
- Evaluar impactos legales
- Evaluar impactos económicos
- Evaluar impactos organizacioneles

Evaluar la efectividad y eficiencia del plan

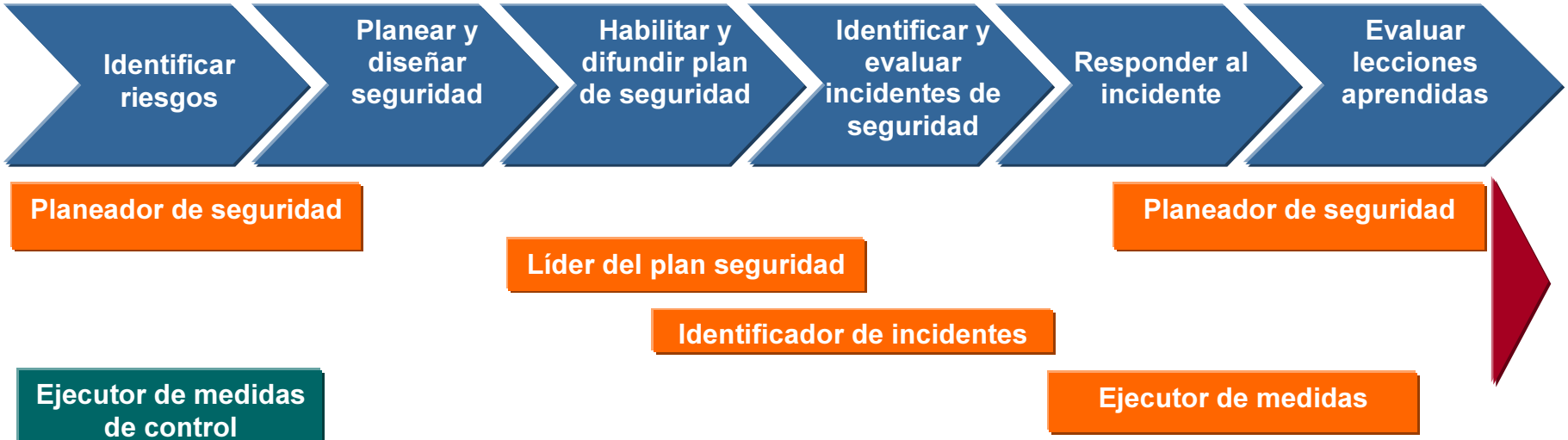
- Analizar la ejecución del plan
- Analizar resultados de la aplicación del plan
- Análisis de brechas y/o áreas de oportunidad
- Documentar lecciones aprendidas

Roles y responsabilidades: Administración de la seguridad



Planeador de seguridad			Líder del plan de seguridad	Identificador de incidentes
• Investigar políticas corporativas, normatividad, Best Practices y reglas de negocio • Estudiar tendencias históricas y lecciones aprendidas • Detectar fallas y/o vulnerabilidad por medio de pruebas • Identificar los esquemas de seguridad actuales • Comparar lineamientos contra los esquemas de seguridad actuales • Determinar impactos tangibles e intangibles y ponderar el impacto del riesgo	• Identificar alternativas legales, tecnológicas, organizacionales y normativas • Evaluar y definir requerimientos, tiempos, costos, dependencias e implicaciones de implantación y operación • Definir estrategia de prevención y/o detección y/o contención y/o recuperación y elaborar el plan de seguridad • Evaluar y predecir la eficiencia y eficacia de la solución propuesta, de acuerdo a los lineamientos (Best Practices, tendencias históricas) • Identificar características del incidente	• Realizar inventario de daños • Evaluar impactos legales, económicos y organizacionales • Analizar la ejecución del plan y sus resultados • Análisis de brechas y/o áreas de oportunidad • Documentar lecciones aprendidas • Realizar pruebas y hacer ajustes • Ejecutar el plan • Capacitación a las áreas involucradas sobre la estrategia de seguridad • Liberar/difundir plan de seguridad	• Gestionar la instalación de barreras de protección y/o perimetrales, equipos, sistemas y servicios • Requerir proyecto de infraestructura de red • Gestionar recursos humanos necesarios • Coordinar las actividades de aplicación del plan	• Monitorear para detectar incidentes (lógico, físico, fraudes y continuidad del negocio) • Recibir reporte de eventos relacionados con la seguridad • Recibir advertencia por entidades externas • Registrar eventos predictibles • Analizar síntomas de incidente • Evaluar impactos al negocio • Determinar la duración del evento • Generar declaración de incidente

Roles y responsabilidades: Administración de la seguridad



- Notificar al grupo encargado de responder al incidente
- Notificar a las áreas que se ven impactadas por el incidente
- Notificar a las autoridades correspondientes
- Ejecutar medidas de contención
- Ejecutar medidas de corrección
- Restaurar condiciones normales de operación

Aplicaciones y sistemas: Administración de la seguridad

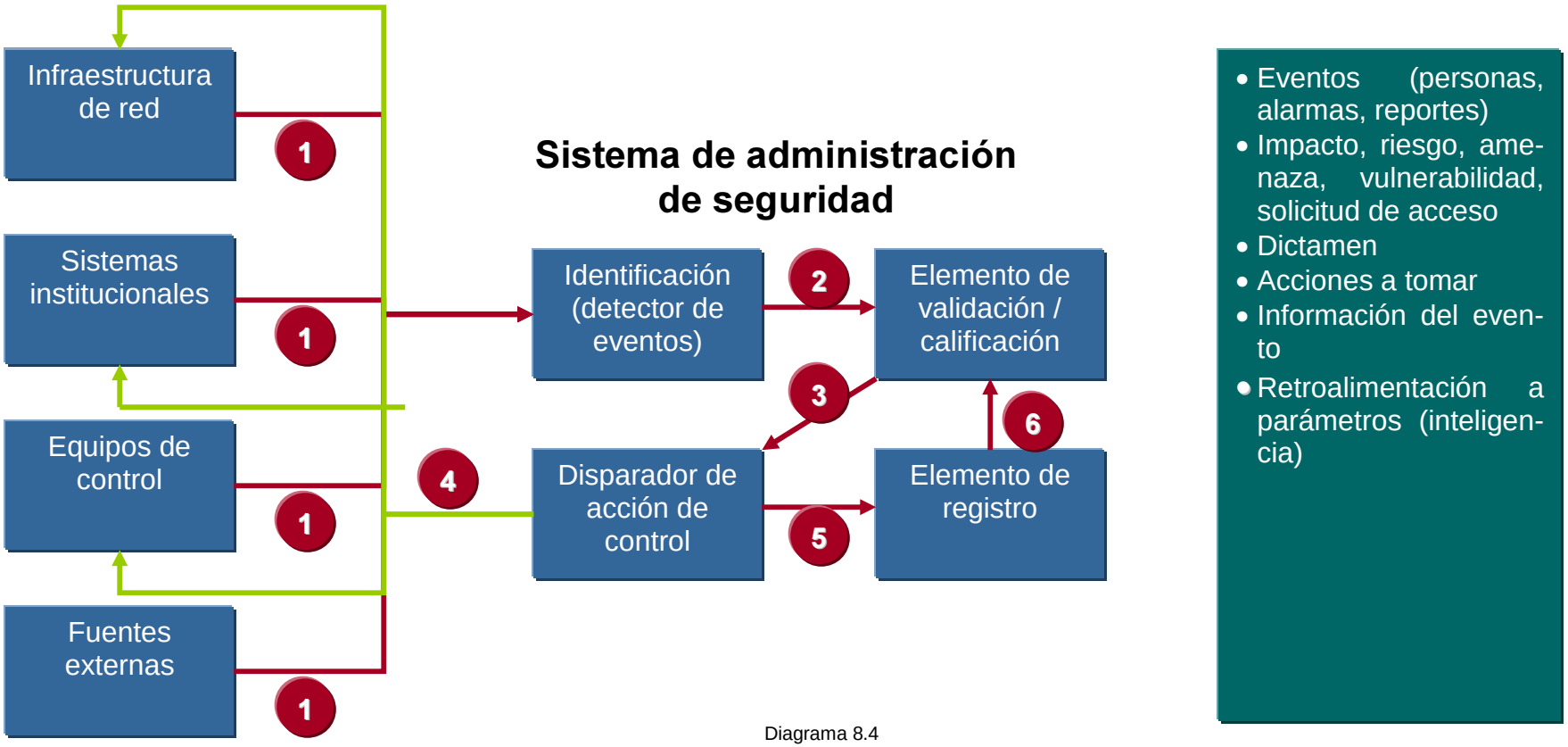


Diagrama 8.4

Nota: La numeración nos indica el flujo de las acciones para manejar las incidencias

En el Diagrama 4 se muestra el flujo de acción que, invariablemente del tipo de incidente hay que considerar para determinar las actividades que se deben desarrollar en el esquema de seguridad informática; lo que nos forzará a detallar y asignar roles que responsabilice al personal de las acciones a seguir.

CAPÍTULO IX
RESULTADOS Y CONCLUSIONES

Resultados

La correcta implantación de controles y selección de éstos es una actividad que deben realizar especialistas en seguridad informática y para esto se requiere de experiencia en ISO 17799 ya que, de no conocerse o trabajarla de forma inadecuada, puede generar seguramente un marco de trabajo estricto y por consiguiente incorrecto para la organización.

Por lo que con este trabajo se pretende ayudar a profesionales que no tienen esta experiencia y que dado el pobre avance en procedimientos aplicados a seguridad informática en México se requeriría de algo alterno, por lo que se propone una metodología a desarrollar, con apego a estándares de calidad, que nos ayude a determina la forma en que debe ser utilizada la ISO 17799, de acuerdo al planteamiento de seguridad informática expuesto en este trabajo.

Los flujos mostrados en los Diagramas 8.1 y 8.2 que han sido detallados en esta propuesta son ejemplo de actividades que se han llevado a cabo en empresas que al carecer de metodologías de seguridad, estructura de seguridad y que al contratar a outsourcers fue necesario realizar, ya que no siempre se cuenta con la implantación de medidas de seguridad y de monitoreos necesarios que faciliten la identificación de incidentes de seguridad, siempre buscando cumplir con niveles de calidad en el servicio interno.

Como ejemplo del éxito de implantación de las metodologías propuestas describimos vivencias en dos empresas, por lo que definiremos como Empresa 1 y Empresa 2.

A continuación se explicará brevemente la forma en se obtuvieron los resultados.

En el caso de la Empresa 1 se tenía en el escenario la necesidad que una empresa llevara el rol de administración de desarrollos, por lo que fue necesario solicitar los servicios de empresas de terceros que llevaran a cabo desarrollos de infraestructura, desarrollos internos, customización de interfases y modificación de módulos de algunas aplicaciones y facturación de éstos. Asimismo, se contrato personal para laborar de forma interna cubriendo después de los desarrollos la operación de éstos; desafortunadamente estas contrataciones no

contaban con la experiencia en metodologías, procedimientos, capacitación y en métodos de seguridad informática ocasionando que se tuvieran deficiencias de administración e implantación de políticas internas, pensando que no sería necesario que se contara con esta experiencia, por lo que, criterios de creación e identificación de perfiles, accesos a Internet, accesos a servidores, aplicaciones importantes de facturación, desarrollos, creación de software, así como, el compartir archivos con información de clientes desde los equipos de cómputo de los empleados, eran actividades que se realizaban sin ninguna restricción, revisión o autorización, aunado a una falta de homologación de configuración de equipos de cómputo tanto laptop como desktop, con un alto riesgo en los accesos a las bases de datos para ejecutar querys por parte de tecnología de información indiscriminadamente, así como personal de facturación, sin tener las facultades correctas, lo que afectaba en la operación, ya que se carecía de una metodología de control de cambios.

Como es notorio, una falta de control y administración de accesos ocasionaba una severidad importante que afectaba a la organización y como consecuencia fuga de información.

La rivalidad con empresas del ramo, la competencia entre sectores, la alta demanda de productos por parte de los usuarios, la falta de concientización de la importancia de la información de nuestros clientes y proveedores obligó a la organización a pensar en el negocio, en la importancia de la información, en los clientes y en trabajar con normatividades y estándares de calidad que permitieran cumplir con las necesidades y obligaciones de servicio necesarias para nuestros clientes y proveedores. De ahí surge la necesidad de realizar un análisis para identificar las vulnerabilidades como primera instancia, así como, el definir las actividades a realizar en lo sucesivo, tal como, el analizar y justificar la inversión y la implantación de procedimientos y políticas internas que fueran claras para la dirección y para los empleados.

Derivado de la operación y al desconocimiento del personal que accedía a aplicaciones en primera instancia se llevó a cabo un levantamiento de actividades e identificación de procesos en toda la empresa. Identificándose,

como era de esperarse, accesos a aplicaciones incorrectos, definición de perfiles erróneos, aplicaciones desconocidas por tecnología de información, actividades y procesos manuales y automatizados que a su vez tenían un grado importante de riesgo dada la información que contenían, como son tarjetas de crédito con datos personales, compras, entre otros. Así pues, después de identificarlas fue necesario crear un grupo de trabajo que se encargara de la administración de aplicaciones, de seguridad interna y del mapeo e identificación del personal vs aplicaciones e interfaces, por lo que se pensó y utilizó la forma de trabajo en el diseño una matriz como la expuesta en este trabajo que permitiera facilitar e identificar el grado de riesgo y la cantidad de personal que accedían a aplicaciones en donde se utilizó la metodología planteada en este trabajo y que permitió reducir los riesgos identificados en su primera fase, así como la pronta atención en caso de incidentes de seguridad o riesgo identificado en el día a día, lo cual dio la base para trabajar con metodologías de seguridad informática, ya que al inicio de estas actividades se carecía de personal certificado y calificado en seguridad permitiendo aun con estas deficiencias el mejorar sustancialmente el desempeño de las aplicaciones, control de accesos, reducción de gastos por la reducción de licencias, se evitó fuga de información con la competencia. Al final de la implantación de las metodologías se logró tener un correcto mapeo de perfiles y de accesos, definición correcta de roles en caso de incidentes de seguridad, tiempos de respuesta a incidentes, lo que permitió posteriormente la implantación de la aplicaciones exitosamente como fue SAP lo que facilitó la implementación de módulos seguridad y de asignación de perfiles, entre otras aunado a una correcta administración de perfiles y accesos a los módulos de SAP así como a las aplicaciones desarrolladas.

Después de la implantación de políticas y restricciones de uso, reducción en la cantidad de perfiles de usuarios, se redujo la cantidad de aplicaciones que no se tenían identificadas, así como identificación de licencias que no habían sido pagadas y perfiles de administración y consulta en las bases de datos.

Algunos ejemplos de las mejoras que se obtuvieron son están en las siguientes tablas:

Implantación de metodología		
Inventario de aplicaciones	Licencias	
	Antes	Después
Windows 2000	2500	3200
Office	2000	3200
Visio	100	300
Siebel	50	100
Infranet	4	10
BD Oracle	300	578
Exchange	2000	3200
Visual Basic	100	400
C++	50	300
ACL	5	20
SAP	20	60
Quest	3	10
GUI	2000	3200

Tabla 9.1

Inventario de licencias de aplicaciones

Implantación de metodología		
Accesos a BD o reportes	Núm. De Accesos	
	Antes	Después
BD Oracle	70	5
BD Seabel	47	5
BD Lotus Notes	20	5

Tabla 9.2

Accesos a bases de datos con perfil de administración

Implantación de metodología		
# de empleados	Carpetas compartidas	
	Antes	Después
3200	1200	100

Tabla 9.3

Información compartida por usuarios

Implantación de metodología	
Antes	
Software sin licencia	#
Windows 2000	700
Office	1200
Visio	200
Siebel	50
Infranet	6
BD Oracle	278
Exchange	1200
Visual Basic	300
C++	250
ACL	15
SAP	40
Quest	7
GUI	1200
iTunes	600
Spayware	50
limeware	120
Plam	100
windvd	70
Juegos	430
winzip	800
Hp Printer	400
Messanger	2344

En el caso de la Empresa 2, desde la década de los 80´s consideró no contar con una planta de personal de sistemas y se decidió el contratar una empresa de outsourcer que administrara las aplicaciones de esta organización. Sin embargo, la cantidad de aplicaciones y la falta de comunicación entre sistemas informáticos, así como la escasa comunicación de las áreas internas en la empresa fue una preocupación para el área de tecnología de información. Contaba con una estructura amplia para atender adecuadamente los desarrollos y necesidades de la empresa, así mismo, al no considerar relacionar la información y la comunicación de sistemas, complicaba la vulnerabilidad de la empresa y de la información, así pues, las áreas operativas tenían su propia forma de administrar los accesos a sus aplicaciones y sus desarrollos internos, dentro de las actividades de tecnología de información se tenía el levantamiento de las necesidades de las áreas y de ahí a la canalización de los desarrollos al outsourcer. Debido a la complejidad de la administración de firmas y recursos, el

alto gasto que implicaba el desarrollar aplicaciones para el control y administración de los accesos fue necesario la comunicación entre áreas en primera instancia y por consiguiente determinar la forma más eficiente de comunicación y automatización de sistemas y aplicaciones, en donde se decidió la utilización de la metodología y herramientas mostradas en este trabajo. Sin embargo, al inicio de esta iniciativa no se contaba con un área interna o la estructura en la organización que permitiera llevar a cabo actividades de seguridad, así como, no se consideró personal con experiencia, personal certificado, capacitado en seguridad informática, se requeriría experimentar un cambio de conceptualización de trabajo y de la propia seguridad informática dentro de la organización, ya que se impedía el tener una adecuada planeación, teniendo como premisa los vicios de personal que tenían más de 15 años de antigüedad, negativa con sindicatos, lo que hacía necesario evaluar el adquirir herramientas que permitieran tener una administración centralizada y supervisada por personal de tecnología de información así como por otras áreas.

Fue necesario llevar a cabo un trabajo de seguridad informática considerando las limitantes de la empresa; por la inversión que esto requeriría se decidió trabajar con la metodología y planteamiento de seguridad informática que se plantea en este trabajo, en esta ocasión propuesto y liderado por auditoría de sistemas en conjunto con tecnología de información. Así fue como se llevó a cabo en primera instancia la definición de roles dada la identificación de aplicación, riesgos, vulnerabilidades y tipo de impacto, así como el monitoreo de aplicaciones y vulnerabilidades obteniendo y trabajando la matriz de riesgos vista en este trabajo, todo esto limitado por el presupuesto con que se contaba, dado el desconocimiento e incertidumbre de los resultados obtenidos se consideró trabajar de forma interna estas necesidad del corporativo. Una vez más fue necesario mapear los procesos, las áreas, las aplicaciones, los costos, los desarrollos, las interfaces, evaluar los desarrollos y funcionalidades al igual que la revisión de procesos manuales y automatizados. Identificando perfiles,

usuarios, accesos y perfil del empleado proporcionado por recursos humanos la definición de estándares de configuración en equipos de cómputo, terminales, etc, así como la determinación de las acciones a seguir en caso de algún incidente de seguridad en donde fue utilizado en primera instancia el flujo de acciones a seguir en caso de incidentes informáticos, determinando roles, identificar y difundir planes de seguridad, responsabilizar de las acciones a seguir en caso de incidentes, respuesta al incidente, lo cual ayudó de forma sorprendente, porque después de implementar las acciones y la definición de roles, se identificó fuga de información y pequeños ataques fueron posibles identificar y tomar acción, con ayuda de otras herramientas fue posible saber cómo se estaba llevando a cabo el ataque, así como el mal uso de las herramientas de trabajo. Lo que trajo como resultado la disminución de gastos al reducir la cantidad de firmas creadas en aplicaciones que incrementaban los gastos y que además ya no eran utilizadas, reducción de anchos de banda. Correcta identificación de firmas por ciudad, reducción de fraudes, ya que distintas personas tenían la misma firma y por cuestiones sindicales no se podía culpar a la persona que realizó el fraude por no garantizar la seguridad de la información y el incumplimiento de políticas internas de la empresa en donde con los procedimientos y documentación se logró el comprometer al sindicato a asumir responsabilidades de sus agremiados por el mal uso de firmas, accesos e información.

Por la falta de conocimiento en las acciones a realizar para impedir fraudes, problemas de imagen, alta incidencia de quejas y compensaciones por mal servicio es necesario implantar procedimientos que evite este tipo de incidentes y de gastos, lo cual también se logró reducir a raíz del uso e implantación de la metodología expuesta en este trabajo, pero sobre todo la forma en que se trabajaban los incidentes de seguridad, ya que se definieron acciones concretas para cada persona que intervenía en cuestiones de seguridad o bien de los accesos de la aplicación, teniéndose una notable mejoría en la organización.

Después de una ardua revisión que llevó casi seis meses, como resultado se obtuvo una oportuna respuesta al incidente, perfecta determinación de las

acciones a realizar para declarar un problema de seguridad, reducción de los tiempos de respuesta, un incremento de servicio de red, servicios dedicados y óptimos accesos a la información como son las bases de datos, mucho menos gastos en la administración de bases de datos ya que los usuarios concurrentes disminuyeron, canalización correcta de los recursos, se dejó de duplicar las acciones y canalizarlas de forma óptima con mucho menos personal dentro de la organización.

De igual forma, la implantación y apego a la metodología permitió reducir la cantidad de incidentes y en lugar de ser reactivos a estos casos se llegó a una proactividad, evitando altos costos de operación, compensaciones improcedentes, mala imagen y mal servicio que en ocasiones son intangibles, pero que al cierre del año se ven reflejados los gastos por errores de seguridad evitándose pérdidas económicas para la empresa, pero sobre todo obteniendo la confianza de los clientes.

Algunos de los resultados obtenidos al trabajar con la metodología se muestran a continuación.

Identificación de firmas y definición de perfiles

APELLIDO	NOMBRE	ID	JORNADA	GS	PD	SU	RC	TR	AS	TA	PR	MA	CE	CIUDAD	ALTA	EMPRESA	AREA	SUBAREA	PUESTO

Irregularidades en infraestructura

Implantación de metodología		
Clasificación	Antes	Después
	# en 6 meses	# finales
Problemas de Red	25	20
Ataques a Firewall	2	5
Ataques a BD	1	15
Apyware	10	50
Mal uso de información	10	100
Accesos a pornografia	5220	45000

Inventario de software

Implantación de metodología		
Software	Antes	Después
	# sin licencia	# con licencia
ACL	5	15
RECOVERY	450	450
O2C	1000	2200
EG	1000	2200
SAP	60	100
Cierres	600	500
FENIX	350	200
JD EDWARS	40	40
PRAS	80	80
DISCOVERY	9	15
PEOPLE SOFT	100	120
Movi Start Edge	0	150
CENTAURO	800	250
PDI	60	140
Windows	1200	3500
WISEVISION	50	20
WINZIP	300	500
SONICSTAGE 3.0	38	0
SCREENSAVER_SPEED_ENG	68	0
QUICKTIME	50	0
PALMONE	80	80
PALM DESKTOP	80	80
MUSICMATCH. JUKEBOX	50	0
MICROSOFT PUBLISHER 2002	20	10
MICROSOFT PROJECT 2000	50	0
MICROSOFT OFFICE VISIO STANDARD 2003	60	0
MICROSOFT OFFICE VISIO PROFESSIONAL 2003	30	90
MICROSOFT OFFICE STANDARD EDITION 2003	500	0
MICROSOFT OFFICE PROJECT STANDARD 2003	65	100
MICROSOFT OFFICE PROJECT PROFESSIONAL 2003	20	0
MICROSOFT OFFICE PROFESSIONAL EDITION 2003	2000	3500
MICROSOFT OFFICE ACCESS 2003	100	50
MICROSOFT OFFICE 97 PROFESSIONAL	5	0
MICROSOFT OFFICE 2000 SR-1 STANDARD	200	0
MICROSOFT OFFICE 2000 SR-1 PROFESSIONAL	200	0
INFORMIX CLIENT SDK	50	50
INFOCONNECT 32-BIT	254	200
EXTRA! PERSONAL CLIENT 32-BIT	300	400
CLIENTE ICA CITRIX	46	46
CITRIX ICA WEB CLIENT	80	120
BLACKBERRY DESKTOP SOFTWARE 4.1	30	30
WINZIP	80	0

Conclusiones

Lograr estándares altamente tecnificados es el reto que se tiene hoy en día y por consiguiente la barrera con la que profesionales debemos trabajar para garantizar la seguridad informática.

Como lo vimos a lo largo de esta propuesta de actividades hay muchos factores que debemos considerar para garantizar la seguridad. La situación internacional actual exige una concientización de la importancia de la información, por lo que hay que trabajar en estándares de servicio teniendo en cuenta la respuesta a incidentes internacionales dado que la información que se puede obtener de parches, actualizaciones, desarrollos, versiones, vulnerabilidades provienen del extranjero, los cuales resultarán de utilidad en la prevención, aunados a los problemas que ya se tienen de forma inherente en la organización, la falta de administración y correcta implantación de los propios sistemas adquiridos hace más compleja la seguridad en la organización, sin embargo puede ser controlable por medio de una ardua labor de administración y concientización de las actividades que se realizan para garantizar la integridad de la información.

Por una parte, cuando se diseña un sistema, erróneamente se desarrolla pensando en su operación y funcionalidad, dejando de lado la seguridad. Por lo que es necesario establecer una correspondencia y pertenencia entre las técnicas adoptadas, conformando un sistema de seguridad con metodología y flujo de actividades perfectamente detalladas.

Existe una infinidad de métodos y herramientas que permite vulnerar un sistema, la red, equipos de cómputo, etc, el encargado de la seguridad o el profesional, debe contar con información y tecnología para la evaluación de incidentes y sólo con metodologías, normas y controles debe garantizar y proteger el interés de la empresa siempre con la constante de la reducción de costos, haciendo esto un reto enorme para el profesional o el experto. De ahí es que se plantea en este

trabajo orientar en la elaboración de procedimientos, en el delego de responsabilidades y en el flujo de actividades en caso de incidentes.

La convergencia de los sistemas expone y multiplica los problemas de seguridad que se puedan identificar, lo que hace necesario enfatizar la necesidad de contar con herramientas, procedimientos, metodologías que nos guíen, nos ayuden a atender los incidentes, vulnerabilidades y fraudes en las empresas y a implementar seguridad en nuestras organizaciones. Es por ello imprescindible desarrollar técnicas y/o adaptar las existentes de forma tal que nuestro trabajo sea conseguir información y adquirir conocimiento dentro de un marco de seguridad como el que se planteó en esta propuesta con los flujos de procesos que se detallaron.

Por otra parte, las tecnologías involucradas en estos procesos condicionan las técnicas empleadas, los tiempos limitan esas tecnologías ya que las legislaciones deben adaptarse a los rápidos cambios que se dan en los sistemas. Esto hace obligatorio no desarrollar procedimientos sobre tecnologías actuales sino sobre conceptos y abstracciones que podrán ser implementados con distintas tecnologías en el presente y futuro, por ejemplo las herramientas como SAP, implementan de forma natural módulos que permite tener niveles de riesgo, controles de acceso y delego de responsabilidad de fácil identificación por TI, auditoría y el administrador en caso de alguna irregularidad, facilitando las labores de control y de integridad de la información, sin embargo mientras esto no se lleve a cabo es necesario trabajar con metodologías como la expuesta .

Es necesario crear políticas internas en la empresa que desaliente acciones futuras en perjuicio de éstas, pero mientras no se den las condiciones que permitan usar metodología y herramientas de seguridad y a sancionar correctamente el abuso de información sin consentimiento del dueño, no se podrán cubrir estándares y problemas de seguridad informática, teniendo como consecuencia gastos, mal uso de servicios, la incertidumbre de usuarios de quien le brinda el servicio, la confiabilidad y alta disponibilidad de nuestra red y de la información.

Conforme se desarrolle y trabaje con flujos de acción a seguir, así como, metodologías de seguridad, se podrá reducir la cantidad de incidentes que se identifiquen, lo que permitirá reducir los gastos de la empresa en desarrollos, administración, incidentes de seguridad y mala imagen.

Bibliografía

- D. Blair, John. Samba, *Integrating Unix and Windows*, Specialized Systems Consultants, Inc. 1998.
- D. McCabe, James, *Network Analysis, Architecture & Design*. Morgan Kaufmann Publishers, Second Edition, USA, 2003
- F.A.Q. de Seg-L *(Lista de seguridad en castellano),* Parte IV, Versión 0.6 - Febrero 1999.
- F. Tipton, Harold and Krause, Micki (eds). *Information Security Management Handbook*. Auerbach Publications, 4th Edition, USA, 2000
- Groth, David. *Network+ Study Guide*. Ed. Sybex, Fourth Edition (N10-003), USA, 2005
- Hiles, Andrew. *Business Continuity: Best Practices: World Class Business Continuity Management.* Rothstein Associates, 2nd Edition, USA, 2004
- McClure, Stuart. *Network Security Secrets & Solutions*. McGraw-Hill, 3rd edition, September 2001.
- Nombela, Juan. *Seguridad Informática*, Ed. Paraninfo, México, D.F. 1996
- Osborne, Hackers 2. *Secretos y Soluciones para la seguridad de redes*. McGraw-Hill, Madrid, 2001
- Reynolds, Janice. *El libro Completo del E-commercer*. Ed. Deusto, España, 2001,
- R. Cheswick, William. *Firewall´s and Internet Security*. Addison-Wesley Publishing Company, USA, April, 1995.
- Schweitzer, Douglas. *Incident Response: Computer Forensics Toolkit*. John Wiley & Sons, USA, 2003
- Stewart, James and Chapple, Mike. *CISSP: Certified Information Systems Security Professional Study Guide*. Sybex, Second Edition, 2004.
- Strebe, Matthew. *Network Security Foundations*. Sybex, USA, 2004
- Tulloch, Mitch. *Microsoft Encyclopedia of Security*. Microsoft Press, 2003
- Velthuis, Piattini. *Auditing Information Systems*. Idea Group Publishing. Hershey, London, 2000
- [Organismos Internacionales]

  ANSI American National Standards Institute
  http://www.ansi.org/

IEEE Transactions on Computer

IEEE Transactions on Communications

The Internet Engineering Task Force
http://www.ietf.org/