UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SERVICIOS OUTSOURCING EN SEGURIDAD INFORMÁTICA

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A N :

ANDRÉS OSVALDO LÓPEZ ROSALES
MARIO ALEJANDRO ROMERO GARCÍA

DIRECTORA: M. C. MARÍA JAQUELINA LÓPEZ BARRIENTOS

MÉXICO, D. F. 2007

AGRADECIMIENTOS

ANDRÉS OSVALDO LÓPEZ ROSALES

A ti Dios que me diste la oportunidad
de vivir y de regalarme una familia maravillosa.

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado
conmigo en todo momento. Los quiero con todo mi corazón.
A mi madre, Julieta, por ser siempre dura pero a la vez tierna.
Y a mi padre, Jorge, por siempre darme ánimos y escucharme.

A Alma Ivette,
tu amor me hace seguir todos los días.
Recuerda que eres mi paz y mi luz.

A mi amigo Alejandro, yo creo que a donde
vayamos siempre hacemos
buena mancuerna.

A mi maestra Jaquelina,
por su gran confianza y gran paciencia.

A mis familiares y a mis amigos de siempre.

A todos los hackers éticos y a todos aquellos que investigan
dentro de la seguridad informática.

Agradecimientos

Mario Alejandro Romero García

A mi mamá, Aida,
que más puedo decir : Gracias por todo

A mi papá, Mario,
por la confianza y apoyo que me ha brindado siempre

A mi hermana, Cynthia,
por su cariño todos los días

A mis abues, Lupita y Samuel,
por compartir conmigo día con día

A mi tía, Laya,
por estar aquí conmigo

A mis tíos, Paquita y Sergio,
por estar siempre al pendiente

A la Maestra, Jaquelina,
por su paciencia y apoyo en este proyecto

A mi colega, Andrés,
teníamos una meta y la logramos

A todos mis amigos y amigas,
a los que se fueron, los que perduran, han sido buenos momentos

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Apéndice

Introducción

Hoy día, son cada vez más las organizaciones que toman conciencia de la importancia de las Tecnologías de Información (TI), para hacer más eficientes sus negocios y mejorar sus operaciones cotidianas. Es necesario establecer que la TI se entiende como "aquellas herramientas y métodos empleados para generar, recabar, retener, manipular y distribuir información". La TI está cambiando la forma tradicional de hacer las cosas; tanto el gobierno, empresas privadas, o un profesional en cualquier campo utilizan la TI cotidianamente.

Esta creciente dependencia conduce a la inminente necesidad de sistemas óptimos que mantengan un tiempo de respuesta adecuado. A raíz de esto nace la seguridad informática, ya que deben protegerse todos los elementos de la red interna de cualquier intento de ataque que puedan preverse y prevenirse, ya sea desde el exterior o desde el interior de la organización.

La seguridad informática, contrario a lo que la mayoría piensa, no consiste simplemente en un producto con alta tecnología; alcanzar un verdadero ambiente de seguridad requiere de personal con conocimiento y experiencia para evaluar y administrar la información de seguridad, procesos claramente definidos y bien establecidos, además de las herramientas apropiadas.

En México, el 99.8% de las empresas son pequeñas y medianas (PyMEs), por ello es necesario encontrar la solución que se ajuste a las necesidades de estas empresas: Servicios de calidad, soporte técnico, experiencia y tecnología de vanguardia, todo esto por un servicio que sea económicamente rentable, consistente y de alta calidad.

Es por esto que el presente trabajo persigue determinar la mejor solución para satisfacer los requerimientos de seguridad de las tecnologías de información de las PyMEs en México.

En el capítulo 1 se establece la importancia de la TI en el desarrollo de las empresas, así como la necesidad de contar con seguridad de los sistemas de TI. Se define el panorama de las PyMEs en México, su actual relación con la seguridad informática y se identifican sus necesidades en seguridad informática.

En el capítulo 2 se describen las estrategias de solución de los requerimientos para la elaboración de un esquema de seguridad informática; se requiere una planeación adecuada que determine cuáles son las vulnerabilidades del sistema a proteger; establecer las políticas de seguridad basándose en normas de todo lo que está y no está permitido hacer; determinar en qué zonas es conveniente instalar dispositivos de seguridad y de qué tipo deben ser éstos. Así, lo primero es identificar los aspectos sensibles, es decir, puntos a proteger dentro de la organización; se clasifica cada uno de ellos con un peso específico y se evalúa la posibilidad de que sea vulnerado, ya sea por ataques intencionados o por causas meramente accidentales.

En el tercer capítulo se establecen los mecanismos necesarios que garanticen la seguridad. Se debe crear una arquitectura tecnológica de seguridad y debe llevarse a cabo un monitoreo de las operaciones y el manejo de la información de seguridad. Este monitoreo se lleva acabo con el uso de herramientas y dispositivos para vigilar el cumplimiento de las políticas, detectar y prevenir incidentes. Sin embargo, el problema que ahora surge, es el gran número de eventos que se generan, los cuales no siempre son importantes; no obstante, se deben revisar. Por lo tanto, no basta con monitorear cada evento, sino que se deben distinguir los relevantes de los que no lo son, por ello se requieren métodos especializados para el monitoreo de la arquitectura de seguridad.

Hemos de tener siempre presente que los riesgos de tener un incidente se pueden minimizar implantando medidas proactivas (aquellas que se toman para prevenir un incidente), pero nunca eliminarlos por completo, por lo que se planificará no sólo su prevención sino también las estrategias de respuesta ante un incidente, también llamadas medidas reactivas (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

En el capítulo 4 se muestra el panorama del outsourcing en materia de seguridad informática. El outsourcing es una estrategia de administración por medio de la cual una empresa transfiere la propiedad y el control de uno o más procesos no críticos a un proveedor altamente especializado para conseguir una mayor efectividad. El objetivo principal del outsourcing es ayudar a las empresas u organizaciones a prever y solucionar conflictos mediante una visión general que permita determinar las prioridades y las principales áreas de oportunidad para mejorar los procesos.

Es por ello que se presenta al outsourcing como una alternativa a la implementación del esquema de seguridad para las PyMEs. Se detalla el perfil de una empresa en el ramo de seguridad informática y se definen los procedimientos para buen desempeño de los servicios.

Finalmente aterrizaremos en el planteamiento de la mejor solución posible para cubrir las necesidades de seguridad de la información a las PyMEs.

Capítulo 1

Relación de las PyMEs con las tecnologías de la información y la seguridad informática

1.1 Importancia de las tecnologías de la información en el desarrollo de las pequeñas y medianas empresas.

1.1.1 La información, recurso de las organizaciones.

Toda organización recoge y analiza datos. Estos datos son de diferentes orígenes y responden a diferentes propósitos: productos, servicios, clientes, agentes, contratistas, proveedores, beneficiarios, costos, insumos, etc.

Un buen indicio del grado de madurez de una organización es el manejo que realiza con los datos. Si se desea maximizar la utilidad de los datos, deben manejarse de forma correcta y eficiente. La utilidad de los datos se materializa en una toma de decisiones correcta y oportuna. Si éstos resultan poco seguros, imprecisos, inoportunos o simplemente están fuera del alcance de quien toma la decisión, el proceso resulta poco confiable.

La información es un conjunto de datos que tienen significado y es considerada hoy como uno de los principales activos de una organización. Los empresarios han comprendido que es un factor determinante para el éxito o fracaso de una empresa u organización.

Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de producción, distribución y almacenamiento de la información manejada en la organización. El implementar un sistema de información en una empresa no garantiza que ésta obtenga resultados de manera inmediata o a largo plazo, debe modificarse y actualizarse con regularidad si se desea percibir ventajas competitivas continuas. Al referirnos a sistemas de información computarizado utilizaremos el término de tecnologías de la información (TI).

1.1.2 Tecnologías de la información, arma básica para la competitividad.

Las tecnologías de información (TI) es un conjunto de computadoras y dispositivos de red conectados para brindar la información en tiempo real teniendo acceso en línea con el objetivo de producir la información correcta para la persona indicada en el tiempo necesario.

La primera generación de computadoras estaba destinada a guardar los registros y monitorear el desempeño operativo de la empresa, pero la información no era oportuna, ya que el análisis obtenido en un día determinado, en realidad describía lo sucedido del día, semana o incluso, del mes anterior.

Los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, tener procesos en línea. Ello obliga a las empresas a pasar de la actual cadena de suministro lineal o secuencial, a una configuración en red donde todos los agentes involucrados participan en los procesos empresariales de forma centralizada.

Hoy día, son cada vez más las organizaciones que toman conciencia de la importancia de las Tecnologías de Información (TI), para hacer más eficientes sus negocios y mejorar sus operaciones cotidianas. Tanto el gobierno, empresas privadas, o un profesional en cualquier campo utilizan la TI cotidianamente. Las tecnologías de la información representan una herramienta cada vez más importante en los negocios. Esto trae consigo otro grupo de estrategias. Utilizando eficientemente la TI se pueden obtener ventajas competitivas, pero es preciso encontrar procedimientos acertados para mantener tales ventajas. Lo que ayuda a una empresa a competir en mejores condiciones no es la tecnología por sí misma, sino su capacidad en beneficio del negocio frente a sus competidores.

La TI es una necesidad para poder sobrevivir en este mundo globalizado, de forma tal, que nos proporcione una ventaja competitiva que produzca un control administrativo sobre los demás recursos de la empresa modernizando operaciones, suministrando una plataforma de información necesaria para la toma de decisiones, reduciendo tiempos, disminuyendo desperdicios y aumentando el nivel de calidad que nos diferencie de las empresas del ramo.

El uso y aprovechamiento de los recursos tecnológicos se han convertido en el factor decisivo para que una empresa, del tamaño que ésta sea, pueda competir y sobresalir. Actualmente, este es el elemento que puede diferenciar a las empresas de su competencia.

1.1.3 Importancia de las pequeñas y medianas empresas en México

En ninguna definición se puede pretender determinar con claridad si una empresa es micro, pequeña, mediana o grande. Existen diversos criterios que nos sirven como parámetros para esta clasificación: número de trabajadores, volumen de producción o ventas, o el valor del capital invertido. En México la clasificación esta basada en el número de empleados y el sector económico que cubren. Publicado en el Diario Oficial de la Federación del día 30 de diciembre de 2002. Ver Tabla 1.1

La participación de las micro, pequeñas y medianas empresas en la economía es fundamental para que exista un crecimiento económico sostenido en el país. De acuerdo al censo económico 2004 del INEGI, el 99.8% son PyMEs. Definitivamente las PyMEs son el motor del desarrollo del país.

	Industria	Comercio	Servicios
Micro	0-10	0-10	0-10
Pequeña	11-50	11-30	11-50
Mediana	51-250	31-100	51-100
Grande	251 en adelante	101 en adelante	101 en adelante

Tabla 1.1 Clasificación de empresas por el número de empleados

Las PyMEs tienen particular importancia para la economía nacional, no sólo por sus aportaciones a la producción y distribución de bienes y servicios, si no también por la flexibilidad de adaptarse a los cambios tecnológicos y gran potencial de generación de empleos. Representan un excelente medio para impulsar el desarrollo económico y una mejor distribución de la riqueza.

Sin embargo, las PyMEs tienen algunas dificultades en virtud de su tamaño: acceso restringido a las fuentes de financiamiento; bajos niveles de capacitación de sus recursos humanos; limitados niveles de innovación y desarrollo tecnológico; baja penetración en mercados internacionales; bajos niveles de productividad; baja capacidad de asociación y administrativa.

De hecho, el acceso al financiamiento ha sido identificado como uno de los más significativos retos para su supervivencia y crecimiento, incluyendo a las más innovadoras. En contraste, las grandes empresas tienen mayor facilidad para obtener financiamiento a través de medios tradicionales debido a que cuentan con mejores planes de negocios, más información financiera confiable y mayores activos.

No obstante sus limitaciones las PyMEs han sido motivo de diseño de políticas encaminadas a promoverlas y apoyarlas para elevar su competitividad y enfrentar la competencia de un mundo globalizado. Han demostrando además que cuando se organizan pueden superar las aparentes limitaciones de su tamaño.

1.1.4 Relación TI y PyMEs en México

La mayoría PyMEs no está familiarizada con el uso de la tecnología ni con soluciones enfocadas a optimizar la operación de su negocio. Sólo tres de cada diez PyMEs mexicanas utilizan TI, lo que toma mayor relevancia al considerar que en México nueve de cada diez compañías se clasifican como PyMEs.

La tecnología de la información es esencial para mejorar la productividad de las PyMEs, aunque su aplicación debe llevarse a cabo de forma inteligente. El hecho de introducir tecnología en los procesos empresariales no es garantía de un aumento de la productividad. Para que la implantación de nueva tecnología produzca rentabilidad hay que cumplir varios requisitos: tener un conocimiento profundo de los procesos de la empresa, planificar detalladamente las

necesidades de tecnología de la información e incorporar los sistemas tecnológicos paulatinamente, empezando por los más básicos.

Las consideraciones a seguir en las PyMEs en cuanto al tamaño de sus recursos informáticos dependerán del número de estaciones de trabajo, carga de procesos, requerimientos de comunicación, usuarios finales, sistemas operativos, software; además de los requerimientos de procesamiento de información actualizada como realizar reportes diarios, de inventarios y de contabilidad. También es necesario considerar el costo, el potencial de crecimiento, soporte técnico y personal.

Las actividades más demandantes son la innovación de esquemas de trabajo, relacionado esto con la forma de manejo, captura y proceso de la información. Quienes ya cuentan con TI requieren que se optimicen los sistemas ya existentes, así como el apoyarse en nuevos programas que agilicen a éstos y enfatizaron finalmente la importancia de la operatividad de la información haciendo uso de Internet.

Algunas oportunidades y áreas de desarrollo que se visualizan y que pueden explorarse y tal vez implementarse en las PyMEs son:

- Incremento en el uso de computadoras. - Promover entre los empresarios de las PyMEs el uso de computadoras, dar a conocer sus beneficios y capacitación en su uso para mejorar la productividad de sus empresas.
- Implementación de redes de computadoras.- Para optimizar el uso del equipo de cómputo y las ventajas del trabajo, se deben implementar redes de computadoras que les permitan además tener contacto con sus clientes y proveedores.
- Aprovechamiento de Internet.- Tomar la experiencia de las PyMEs de otros países que han utilizado y explotado Internet para su publicidad y transacciones comerciales, que les han permitido comprar y vender sus productos a otras partes del mundo.
- Desarrollo de Software a la medida.- Aprovechar las herramientas de productividad comerciales y desarrollar aplicaciones de software acorde a la organización.
- Capacitación del personal de las empresas.- Crear y diseñar cursos de capacitación al personal de las PyMEs en el uso y aplicación de las TI que mejoren la productividad de las empresas y darles herramientas para que sean competitivas a nivel nacional e internacional.

Las PyMEs para implantar las nuevas tecnologías se ven en la necesidad de contratar especialistas en TI. Pues éstos realizan una evaluación de las necesidades de tecnología factibles para la empresa. Las áreas importantes a considerar por éstos especialistas para implantar TI son:

- Planeación, colaboración y toma de decisiones corporativas
- Finanzas y administración

- Producción y Operaciones
- Gestión del abastecimiento (relación con proveedores)
- Mercadotecnia, conocimiento y relación con los clientes
- Ventas y distribución
- Desarrollo y mejora de productos y servicios

Las PyMEs serán más competitivas con el uso y apoyo de las TI, por lo que aportarán más al PIB, se incrementará la tasa de empleo debido a la expansión de estas empresas, en general, se dará un impulso a la economía.

Según un estudio desarrollado por la unidad de inteligencia de The Economist, en el año 2010 para las empresas será más importante la manera de hacer negocios, que el servicio o producto al que estén dedicados. El 54% de los que respondieron a una encuesta global de 4,000 ejecutivos de alto nivel, que se llevó a cabo entre noviembre del 2004 y enero del 2005, los nuevos modelos de negocios serán la verdadera fuente de la ventaja competitiva en el 2010 y más importante que los nuevos productos o servicios que puedan desarrollar.

Los productos o servicios serán importantes, pero cada vez más vulnerables y susceptibles de ser replicados. Un cambio en el modelo de negocios, sobre como son los productos creados, entregados y mantenidos, marcará la diferencia y se traducirá en una ventaja competitiva. La tecnología estará en el corazón de los esfuerzos para llegar a esto. Los avances en la tecnología tendrán la mayor influencia en el lapso 2005-2010 sobre los modelos de negocios fue la opinión del 41% de los que respondieron a la encuesta. Y fue el 87% los que afirmaron que son las tecnologías de la información el punto crítico para que sus empresas puedan adaptar sus modelos de negocio y desarrollar estrategias e incrementar así su competitividad.

1.2. Importancia de la seguridad de los sistemas de TI.

1.2.1 Seguridad informática, una necesidad actual.

Hoy día uno de los principales activos de cualquier empresa, es la información contenida en sus sistemas informáticos. Dicha información es susceptible de ser perdida por errores no intencionados de los usuarios; robada, destruida, modificada o deteriorada por ataques o códigos maliciosos, por lo tanto, debe ser protegida.

A raíz de esto nace la seguridad informática con el fin de salvaguardar y satisfacer las necesidades de operación. La seguridad informática se refiere a la protección de sistemas de información contra accesos no autorizados o a la modificación de información. Protegerla durante su almacenamiento, procesamiento y tránsito, tener información en la cual se pueda confiar, preservar la privacidad de la información, asegurar que los datos permanezcan inalterados durante su transmisión, asegurar que un usuario está en comunicación con la persona con quien cree estarlo, garantizar que solamente los usuarios autorizados tienen acceso a los recursos de la infraestructura y garantizar la disponibilidad de la información para los usuarios autorizados, cuando y desde donde lo requieran.

1.2.2 Conceptos básicos de seguridad informática.

Podemos definir la seguridad informática como el conjunto de normas, políticas, procedimientos, estándares mínimos que deben ser considerados en el desarrollo, implementación y operación de los sistemas y servicios informáticos, con la finalidad de garantizar la integridad, confidencialidad, autenticación y disponibilidad de la información (CIA por sus siglas en inglés, Confidenciality, Integrity and Aviability).

1.2.2.1 La Triada de la Seguridad CIA-AAA

Los conceptos esenciales que deben conocerse para la implementación de un sistema de seguridad son:

Confidencialidad

Se define como servicio de seguridad que asegura que la información no pueda estar disponible o ser descubierta por otras personas, entidades o procesos no autorizados. Se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

Integridad

Característica que asegura que la información es genuina, completa y exacta, garantizando su protección contra una modificación no autorizada y/o

accidental. Los cambios serán realizados por personas autorizadas. Significa que el sistema no permitirá a alguien no autorizado modificar o corromper la información que almacene, procese o transmita. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado.

Disponibilidad

Un sistema seguro debe mantener la información disponible para los usuarios, que el sistema, tanto hardware como software, se mantengan funcionando eficientemente en el momento que se requiera, cuantas veces sea necesario y con capacidad de recuperación rápida en caso de fallo. Garantizar que los sistemas trabajen adecuadamente y que el servicio no sea negado a usuarios autorizados.

La autenticación, autorización y la auditoría (AAA) son una serie de procesos usados para garantizar la CIA.

Autenticación

Es el proceso de identificación de un usuario (programa o dispositivo), normalmente mediante un nombre de usuario y contraseña, un token o un biométrico. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

Autorización

Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.

Auditoría

Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, tiempo de conexión así como los datos transferidos durante la sesión. Los datos registrados se utilizan con fines estadísticos en materia de seguridad sobre dispositivos, aplicaciones, usuarios, transacciones y mensajes.

1.2.2.2 Mantener la TI, reto de la seguridad

La seguridad informática tiene como reto, mantener en todo momento la CIA-AAA, pero existen circunstancias que tratan de poner en peligro estas propiedades de la información:

Amenaza

Un evento o actividad con el potencial de causar un daño a nuestras TI.

Vulnerabilidad

Es una debilidad o hueco de seguridad que puede ser explotada por una amenaza, causando un daño. Puede ser causada por una mala configuración.

Riesgo

La posibilidad de que una amenaza se lleve a cabo. Por lo que, los riesgos son todas aquellas acciones que supongan una violación de la seguridad.

1.2.2.3 Ataques, incidentes de seguridad

Al tratar de explotar una vulnerabilidad, una amenaza se convierte en un ataque. Los cuales crean incidentes y tienen un impacto hacia nuestra infraestructura de TI.

Incidente

Cualquier evento que no forma parte de la operación normal y daña o puede dañar la confidencialidad, integridad y disponibilidad de la operación y de la información.

Ataque.

Acción deliberada que atenta contra los sistemas de seguridad. Violación a las políticas de seguridad que deriva de una amenaza.

Se puede categorizar a los ataques de la siguiente manera:

- *Interrupción*: Un recurso del sistema es destruido o se vuelve no disponible. Éste es un ataque contra la disponibilidad. Ejemplos de este ataque son los de negación de Servicios (DoS), que causan que los equipos queden fuera de servicio.
- *Intercepción*: Una entidad no autorizada consigue acceso a un recurso. Éste es un ataque contra la confidencialidad. Ejemplos de este ataque son la obtención de datos mediante el empleo de programas troyanos o la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes de datos para desvelar la identidad de uno o más de los usuarios mediante el "*Spoofing*" o engaño implicados en la comunicación intervenida (intercepción de identidad).
- *Modificación*: Una entidad no autorizada no sólo consigue acceder a un recurso, si no que es capaz de manipularlo. Virus y troyanos poseen esa capacidad. Éste es un ataque contra la integridad. Ejemplos de este ataque son la modificación de cualquier tipo en archivos de datos, alterar un programa para que funcione de forma distinta y modificar el contenido de información que esté siendo transferida por la red.
- *Fabricación*: Una entidad no autorizada inserta objetos falsificados en el sistema. Éste es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir datos a un archivo.

Por el lugar donde se generan los ataques se pueden clasificar en: internos y externos

Ataque interno

Pérdida de información que proviene de la acción de empleados descontentos o antiguos trabajadores despedidos por sus empresas, con fines de lucro o con el único aliciente de fastidiar deciden robar o destruir la información.

Existen numerosos casos de empleados que se apropian de documentos, archivos, o roban clientes de la cartera comercial, pretenden utilizar el trabajo realizado, como puede ser el desarrollo de una aplicación informática innovadora en el mercado, para utilizarlo y establecer su propio negocio.

Ataque externo

Son todos aquellos que se generan desde fuera de la infraestructura o por personal ajeno a la organización. Usuarios mal intencionados, intromisiones al sistema, código malicioso (virus, gusanos, troyanos) son algunos ejemplos de riesgos externos.

Recientes investigaciones del CERT han encontrado que el 70% de los problemas de seguridad informática provienen desde el interior de la empresa u organización, causados por el personal que labora dentro de ellas.

El siguiente gráfico detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos. Ver Figura 1.1

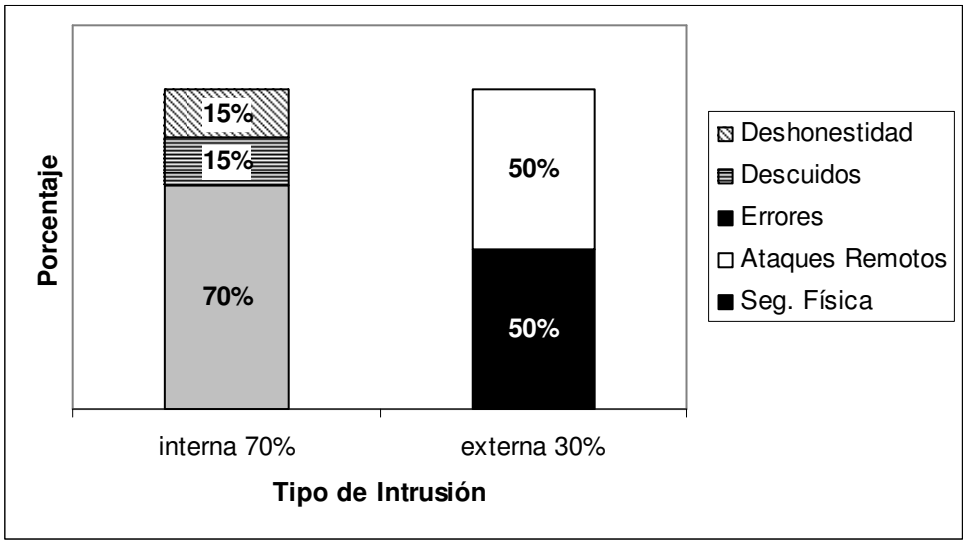


Figura 1.1 Porcentaje de intrusiones

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque

realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar.

Asimismo los ataques se pueden clasificar en pasivos y activos.

Ataques pasivos

El atacante no altera la comunicación, únicamente la escucha o monitoriza, para obtener la información que está siendo transmitida.
La intercepción de datos y el análisis de tráfico se pueden realizar mediante:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

Ataques activos

Implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos; pueden dividirse en cuatro categorías:

- *Suplantación de identidad*.- El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- *Modificación de mensajes*.- Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
- *Degradación fraudulenta del servicio*.- Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes. Entre estos ataques se encuentran los de denegación de servicio.
- *Reactuación*: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Ahora veamos los modos de ataques:

Escaneo de puertos

Consiste en buscar puertos abiertos y fijarse en los que puedan ser receptivos o de utilidad. El escaneo tradicional consiste en seleccionar un rango de IPs y hacer esas "llamadas" a unas direcciones IP consecutivamente, aunque también se puede hacer un escaneo a una IP concreta. Los firewall actuales detectan esa llamada a puertos consecutivos y por lo tanto reconocen el escaneo. Así que se cambia el método y se escanean las IPs y los puertos de cada una de ellas de forma no consecutiva. También se puede intentar cambiar el método de comunicación entre ambas máquinas.

Ataques de Autenticación

Consisten, como su nombre indica, en la suplantación de una persona con autorización por parte del atacante. Se suele realizar de dos formas: obteniendo el nombre y contraseña del atacado o suplantando a la víctima una vez ésta ya ha iniciado una sesión en su sistema.

Simulación de identidad

Es una técnica para hacerse con el nombre y contraseña de usuarios autorizados de un sistema. El atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta entrar en él teclea su login y password, el programa los captura y muestra una pantalla de "error en el acceso" al usuario. El usuario vuelve a teclear su login y password, entrando esta vez sin problemas. El usuario cree que en el primer intento se equivocó al teclear, sin embargo, su login y password han sido capturados por el atacante.

Spoofing

Engaño. Este tipo de ataques suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Consiste en sustituir la fuente de origen de una serie de datos (por ejemplo, un usuario) adoptando una identidad falsa para engañar a un firewall o filtro de red. Los ataques Spoofing más conocidos son el IP Spoofing, el DNS Spoofing , el Web Spoofing y el fake-mail.

Looping

El intruso usualmente utiliza algún sistema para obtener información e ingresar en otro, que luego utiliza para entrar en otro, y así sucesivamente, tiene como finalidad hacer imposible localizar la identificación y la ubicación del atacante, perderse en la red.

IP Splicing-Hijacking

Es un método de sustitución que consiste en que el atacante espera a que la víctima entre en una red usando su nombre, contraseña y demás y una vez que la víctima ha superado los controles de identificación y ha sido autorizada la saca del sistema y se hace pasar por ella.

Utilización de Backdoors (Puertas Traseras)

Son trozos de código en un programa que permiten a quien los conocen saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. No es por tanto un método de suplantación, si no de saltarse los controles de autentificación o, como su nombre indica, entrar por la "puerta de atrás". Son fallas de seguridad que se mantienen, voluntariamente o no, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

Exploits

Es muy frecuente ingresar a un sistema aprovechándose de vulnerabilidades en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrado un error en los programas utilizados.

Obtención de Contraseñas

Es la obtención por "Fuerza Bruta" de nombres de usuarios y claves de acceso. Casi todas las contraseñas que utilizamos habitualmente están vinculadas a nuestros nombres reales, nombres de familiares y/o mascotas, fechas significativas, etc. Además, no las solemos cambiar periódicamente. También se suele realizar este tipo de ataques usando una clase de programas llamados diccionarios.

Denial Of Services (DoS)

Ataque de negación de servicio. Se impide a la víctima de acceder y/o permitir el acceso a un recurso determinado. Por ejemplo, no puede conectarse, usar el correo electrónico o, a un mayor nivel, obstaculiza a un servidor de prestar sus servicios. Se basa en el hecho comprobado de que es más fácil corromper un sistema que acceder clandestinamente al mismo. Estos ataques intentan corromper o saturar los recursos de la víctima por medio de peticiones de conexión para lograr desactivarla o impedir el acceso a otros usuarios por medio de la saturación. Ejemplos de este tipo se han visto cuando se atacó al servidor DNS de Terra, o el sitio de www.sco.com recientemente.

Mail Bombing-Mail Spamming-Junk Mail (correo basura)

El Mail Bombing consiste en un envío indiscriminado y masivo de un mensaje idéntico a una misma dirección, saturando así buzón de correo (mailbox) del destinatario. El Mail Spamming en cambio es un bombardeo publicitario que consiste en enviar un correo electrónico no solicitado o no deseado a miles de usuarios. Es muy utilizado por las empresas para publicitar sus productos. Generalmente, suelen ser: publicidad, ofertas o enlaces directos una página web. Estos mensajes son enviados a cientos de miles de destinatarios cada vez. El correo basura roba recursos del sistema. Su distribución causa la perdida de ancho de banda en la Red, y multiplica

el riesgo de infección por virus. Las personas o empresas que envían este tipo de emails, construyen sus listas usando varias fuentes. Normalmente, utilizan programas que recogen direcciones de correo desde Usenet, o recopilan las mismas de otras listas de distribución. Muchos de los mensajes no solicitados nos ofrecen la opción de eliminarnos. La experiencia demuestra que este método es una trampa, y que sólo sirve para verificar que la dirección de correo existe realmente, y se encuentra activa. Por otro lado, si respondemos alguno de estos emails, el resultado es idéntico, seremos colocados automáticamente en una nueva lista de distribución, confirmando nuestra dirección.

El Spamming esta siendo actualmente tratado por las leyes europeas como una violación de los derechos de privacidad del usuario.

1.2.2.4 Código Malicioso

Definiremos a continuación las principales amenazas surgidas por código malicioso:

Virus

Es un pequeño programa capaz de reproducirse a sí mismo, infectando cualquier tipo de archivo ejecutable, sin conocimiento del usuario. El virus tiene la misión que le ha encomendado su programador, ésta puede ser desde un simple mensaje, hasta la destrucción total de los datos almacenados en el ordenador. Se llaman de esta forma, por su analogía con los virus biológicos del ser humano. Al igual que estos, los informáticos tienen un ciclo de vida, que va desde que "nacen", hasta que "mueren". Creación, gestación, reproducción, activación, descubrimiento, asimilación, y eliminación. Además, existen varias técnicas que permiten a un virus ocultarse en el sistema y no ser detectado por el antivirus: ocultación, protección antivirus, camuflaje y evasión.

Gusanos

Es un código maligno cuya principal misión es reenviarse a sí mismo. Son códigos víricos que, en principio, no afectan a la información de los sitios que contagian, aunque consumen amplios recursos de los sistemas, y los usan para infectar a otros equipos aprovechando bugs de los sistemas a los que conecta para dañarlos. A diferencia de la mayoría de virus, los gusanos se propagan por sí mismos, sin modificar u ocultarse bajo otros programas. No destruyen información de forma directa, pero algunos pueden contener dentro de sí, propiedades características de los virus. El mayor efecto de los gusanos es su capacidad para saturar, e incluso bloquear por exceso de tráfico los sitios web, aunque estos se encuentren protegidos por un antivirus actualizado.

Un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras

que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa; tiempo más que razonable para detectarlo, un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

Troyanos (caballos de troya)

Es un programa potencialmente peligroso que se oculta dentro de otro para evitar ser detectado, e instalarse de forma permanente en nuestro sistema. Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información privada, enviándolos a otro sitio. Otra de sus funciones es dejar indefenso nuestro sistema, abriendo brechas en la seguridad, de esta forma se puede tomar el control total de forma remota, como si realmente se estuviera trabajando delante de nuestra pantalla.

Spyware

Los programas espía se instalan en un ordenador sin el conocimiento del usuario, para recopilar información del mismo o de su ordenador, enviándola posteriormente al que controla dicha aplicación. Existen dos categorías de spyware: software de vigilancia y software publicitario. El primero se encarga de monitorizar todo el sistema mediante el uso de transcriptores de teclado, captura de pantallas y troyanos. Mientras, el segundo, también llamado "Adware", se instala de forma conjunta con otra aplicación o mediante controles ActiveX, para recoger información privada y mostrar anuncios. Este tipo de programas registran información sobre el usuario, incluyendo, contraseñas, direcciones de correo, historial de navegación por Internet, hábitos de compra, configuración de hardware y software, nombre, edad, sexo y otros datos secretos. Al igual que el correo basura, el software publicitario, usa los recursos de nuestro sistema, haciendo que sea este el que pague el coste asociado de su funcionamiento. Además, utiliza el ancho de banda, tanto para enviar la información recopilada, como para descargar los banners publicitarios que nos mostrará.

1.3. Panorama de las PyMEs y su actual relación con la seguridad informática.

1.3.1 Panorama internacional de la seguridad informática

Según datos estadísticos de la Computer Security Institute, organismo líder mundial en materia de informática y sistemas de seguridad, las empresas en los Estados Unidos sufrieron algún tipo de incidente de seguridad durante el 2005 que causaron pérdidas por 130 MDD. Podemos observar en la Figura 1.2 que el mayor índice fue ocasionado por la propagación desmesurada de virus. En este caso, existe una clara relación entre el número de incidentes y los daños causados a las empresas. Sin embargo, esta relación no se existe en los demás tipos de incidentes. De ello podemos deducir que existen incidentes que se presentan poco pero causan fuertes pérdidas económicas y viceversa.

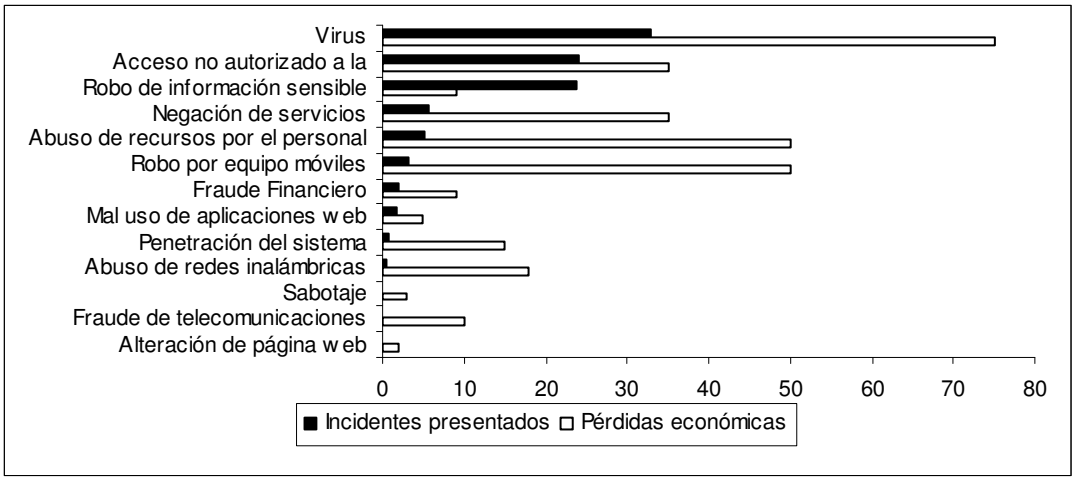


Figura 1.2 Relación entre incidentes presentados y pérdidas económicas (Porcentajes)

Podemos observar en la figura que los accesos no autorizados a la información, robo de información sensible y el abuso de recursos, todos estos relacionados con el personal; en conjunto causan mayores pérdidas económicas que los virus. Datos obtenidos en el mismo estudio, nos muestra los índices de uso de diferentes soluciones tecnológicas de seguridad. Ver Figura 1.3

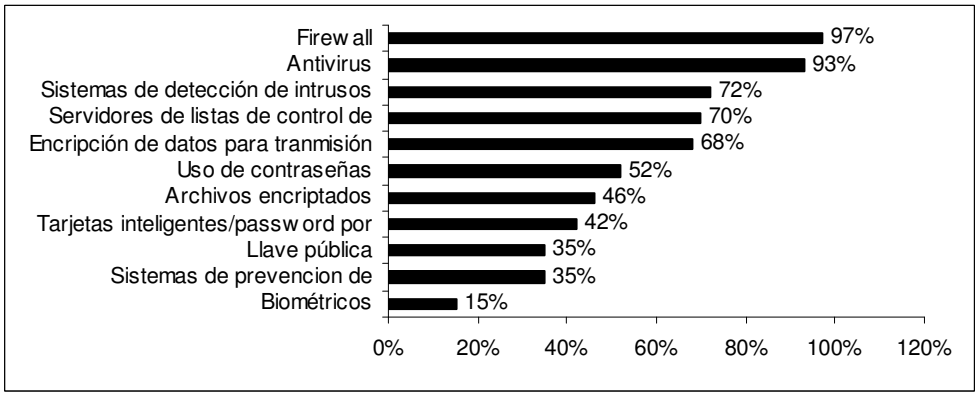


Figura 1.3 Índice de uso de diferentes soluciones tecnológicas de seguridad (Porcentajes)

1.3.2 Panorama en México de la seguridad informática

Encuestas realizadas por Ernst & Young, firma internacional dedicada a la consultaría de negocios, nos presentan los incidentes que se registraron en México durante el 2003. Del total de incidentes registrados, el 24.4% fue provocado por código malicioso y se presentó en el 75% de las empresas. Ver figura 1.4

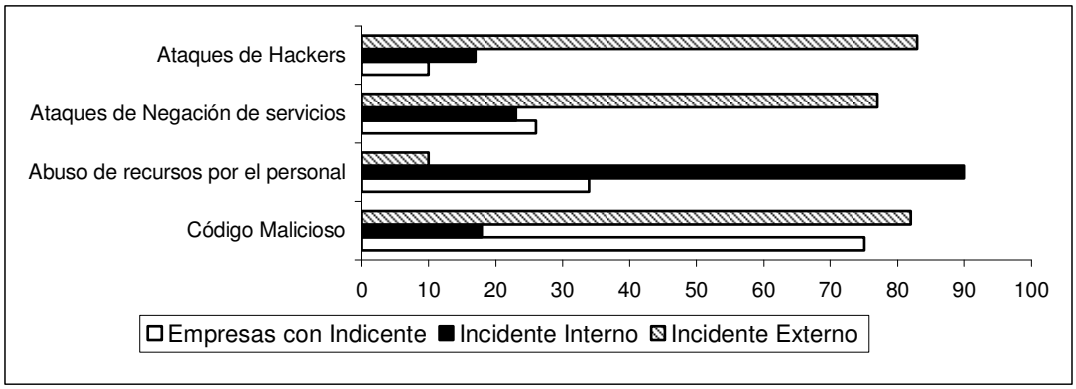


Figura 1.4 Incidentes ocurridos en México durante el 2003 (Porcentajes).

Con base en esto, los empresarios buscan estrategias de seguridad para contrarrestar los incidentes. La tabla 1.2, nos muestra las prioridades para implementar tecnologías de seguridad contra los diferentes incidentes. Sin embargo, las principales dificultades para el éxito en la aplicación de sistemas de seguridad informática son las limitaciones presupuéstales, la dificultad para demostrar la importancia de la seguridad de la información y la falta de conciencia en los ejecutivos y usuarios. Normalmente, los recursos son asignados de forma reactiva y no proactiva. Es decir, solo se toma conciencia de la seguridad informática y se asignan recursos una vez que ya han sufrido de algún incidente, y no para prevenirlos.

Prioridad	Tipos de incidentes
Alta	1. Códigos maliciosos (virus, gusanos y troyanos) 2. Abuso de los recursos por el personal
Media	3. Negación de servicio 4. Seguridad física 5. Spam 6. Mal uso de los recursos de terceros (clientes y proveedores) que tengan acceso a la infraestructura de TI 7. Perdida o robo de datos
Baja	8. Cumplimiento de normas y reglamentos 9. Desastres naturales 10. Hackeo

Tabla 1.2 Prioridades contra tipos de incidentes

1.3.3 Panorama en PyMEs de México en relación con la seguridad Informática

Comúnmente se piensa que quién necesita de la seguridad informática son organismos, instituciones o empresas que:

- Manejan información confidencial, especializada o que requiere un manejo delicado, y deben mantener una imagen de seguridad frente a sus clientes. Entre ellas están las instituciones bancarias y las dependencias gubernamentales.
- Administran información relevante con ayuda de las tecnologías de la información, tales como las del sector industrial.
- Ofrecen sus servicios, o parte de ellos, a través de internet y por tanto, dependen del buen funcionamiento de sus sitios web.

La realidad es otra. En toda organización que haga uso de TI se recomienda implementar seguridad; no importa el tipo, giro o tamaño de la organización; ya sea una institución gubernamental, una Pyme o un conglomerado multinacional; todos requieren que se les proporcione un servicio de seguridad informática que les de la tranquilidad de saber que están protegidos frente a posibles ataques, un servicio que garantice la confidencialidad, integridad y disponibilidad de la información; que sus vulnerabilidades críticas sean detectadas y reparadas, que disminuya el riesgo de fuga de información, así como de impactos por virus o hackeo. Es preciso mantenerse al tanto de las últimas actualizaciones para protección, ya que todos los días surgen nuevos tipos de ataques y modos de contrarrestarlos. El objetivo de la seguridad es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de la información. Todo esto por un servicio que sea económicamente rentable, consistente y de alta calidad.

En las PyMEs existen oportunidades donde la seguridad de las tecnologías de información puede implementarse, solo que el presupuesto y ante todo, el desconocimiento de su importancia han frenado su desarrollo.

Más que un gasto tecnológico, los recursos que una empresa destina a este rubro deben ser vistos como una inversión, ya que a la larga le da mayor rentabilidad a las empresas. La seguridad informática es una decisión de negocio, ya que cualquier incidente por mínimo que sea puede afectar la operación y los ingresos de las compañías.

CAPÍTULO 2

Identificar las necesidades y estrategias de solución de la seguridad informática

2.1 Identificar las necesidades en seguridad informática de las PyMEs.

2.1.1 La información, el activo principal

En la operación diaria de un negocio se toman decisiones, la mayor parte de éstas son tomadas con información. Desgraciadamente en gran número de las pequeñas y medianas empresas (PyMEs) no existe una sola fuente de información, sino diversos sistemas informales en los se basan para tomar decisiones que inciden en la operación de sus negocios, en caso de ser erróneos pueden tener un fuerte impacto económico en la empresa.

El primer paso para tener una administración basada en información es tener una sola fuente, si existen diversas fuentes siempre se van a dedicar inútilmente recursos a que la información cuadre, o se dedicará un doble esfuerzo para mantener actualizados ambos sistemas; es conveniente tener una sola fuente de información, con información buena o mala, pero que al menos sea la misma para todos.

Una vez logrado este primer paso, el segundo paso es cerciorarse que esta fuente única de información, tenga la información correcta; el sistema debe reflejar la realidad de lo que está pasando en la empresa.

La información para que sea útil debe tener estas características:

- Exactitud.- Reflejar lo que está pasando en el negocio.
- Totalidad.- Contar con toda la información crítica para el negocio.
- Oportunidad.- Disponible cuando se requiere para tomar una decisión.
- Relevancia.- Que sirva a la persona a quien se le está proporcionando.
- Consistencia.- Que sea la misma en todas las áreas de la compañía.
- Nivel.- Dependiendo del nivel organizacional y al tipo de decisión al cual esté destinada la información.

Toda la información mantenida por una Pyme tiene un valor tangible e intangible, como aquella que ha sido desarrollada dentro de la compañía o comprada. La compañía deberá decidir la restricción al acceso a dicha información si determina que el acceso no autorizado pudiera disminuir el valor de la información, proporcionar ventaja a la competencia o violar obligaciones legales debido a la divulgación; por ejemplo, análisis de mercado, proyecciones de ventas, investigación y desarrollo de tecnología de vanguardia.

El tercer paso es resguardar la información y así obtener mejores resultados para el negocio, ya que esto mejorará la eficiencia de los procesos, lo cual muchas veces conduce a menores costos del mismo y elevará la calidad de la prestación del servicio o manufacturación de un producto.

Para protegerla debe adoptarse un enfoque consciente y bien planeado. Requiere de recursos como tiempo y dinero. Existen muchos costos asociados con la implementación de un sistema de seguridad: costos de capacitación, compra de sistemas y herramientas nuevas o actualizadas y muy posiblemente el uso de consultores externos.

El objetivo no es tan solo proveer seguridad, sino el de apoyar a la organización a hacer buen uso de la información para mejorar el uso de los recursos y las operaciones del negocio.

2.1.2 Distinguir la información crítica para el negocio.

En ocasiones existe tanta información que difícilmente podemos dedicar suficientes recursos, por lo que hay que determinar cuál es la información que tiene un mayor impacto en las operaciones del negocio. Establecer dónde se encuentran los mayores problemas y priorizar las áreas con las que hay que iniciar el esfuerzo.

Muchas organizaciones encuentran cuatro categorías para identificar y agrupar la información con base en su grado de sensitividad, estas categorías son enlistadas en orden ascendente de sensitividad en la tabla 2.1.

Tipo de Información	Descripción
Pública	Apropiada para su divulgación al público en general a través de noticias, o documentos públicos. En esta información puede estar la clave del éxito de la organización o un proyecto. Dirigida a clientes y proveedores.
Sensitiva	Disponible únicamente para los empleados de la organización, más no para el público en general. La pérdida de esta información pudiera proporcionar ventaja a la competencia o desconcertar a la organización si es revelado en una manera no apropiada. Ejemplos: planes generales de un producto especifico o una base de datos en que se han invertido demasiados recursos para su desarrollo.
Restringida	Limitada a cierto sector del personal. La entrega o descubrimiento de este tipo de información puede resultar en una variedad de daños, desde pérdida de confidencialidad de un cliente hasta el sabotaje de planes estratégicos. Ejemplos: Investigación y desarrollo de datos asociados con un plan estratégico, parámetros de seguridad de un software o claves de acceso para un equipo.
Secreta	Disponible para un número limitado de usuarios. El acceso deberá ser controlado utilizando bitácoras de firmas supervisadas generalmente por el propietario de la información. Dirigida a miembros de dirección.

Tabla 2.1 Clasificación de la información

Dependiendo del entorno, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un proceso de manufactura se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial que se podría recuperar después desde una cinta de respaldo, a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados. En cambio, en alguna base de datos de un departamento se premiará la disponibilidad frente a la confidencialidad: importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero. En un entorno monetario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

Es necesario establecer parámetros para determinar nuestro nivel de seguridad. Lo que no se puede medir no se puede administrar y no se puede mejorar. Estos medidores deben estar al alcance de las personas que serán las responsables de monitorear y determinar las posibles causas de fallos; se definirán planes de acción encaminados a la mejora continua.

2.1.3 Amenazas

Las amenazas son todo aquello que intenta o pretende destruir nuestro sistema y para ello puede explotar los fallos de seguridad que denominamos vulnerabilidades y como consecuencia, causar incidentes que originen impactos que impliquen pérdidas o daños a la empresa. Ver Figura 2.1

Figura 2.1 Relación Amenaza-Incidente-Impacto

Las amenazas se pueden convertir en realidad a través de fallas de seguridad, por tanto éstas deben ser contrarrestadas al máximo para que el ambiente que se desea proteger esté libre de riesgos de incidentes de seguridad. Por lo tanto, la relación entre amenaza-incidente-impacto, es la condición principal a tomar en cuenta en el momento de priorizar acciones de seguridad para la corrección de los activos que se desean proteger y deben ser siempre considerados cuando se realiza un análisis de riesgos.

Dada la importancia de las amenazas y el impacto que puede tener para la información de las organizaciones, revisemos ahora su clasificación. Tabla 2.2

Amenazas		Descripción
Naturales	**Fuego, Terremotos, Tornados, Inundaciones, entre otros**	Condiciones de la naturaleza que podrán causar daños a los activos, tales como fuego, inundación, terremotos. Son las menos probables al menos en comparación con el riesgo de sufrir un intento de acceso no autorizado o una infección por virus. Sin embargo, no implica que no se tomen medidas básicas contra ellas, ya que si se produjeran generarían daños mayores.
Físicas	**Hardware**	Cualquier dispositivo de red, ya sea un router o un simple cable, una impresora, un servidor, el firewall, una maquina, su tarjeta madre o la tarjeta de red, alguna interfaz o su procesador son susceptibles a fallos.
	Software	Una gran cantidad de sistemas operativos o aplicaciones sacan actualizaciones para agregar características y proporcionar mejoras a la funcionalidad el producto o cerrar vulnerabilidades de seguridad que se han descubierto. Es necesario estar al día e incluso, si es posible, instalar éstas de manera automática. Cualquier software, ya sea comercial, con actualizaciones o sin ellas, desarrollado por la misma organización o no, es susceptible a fallos.
Humanas	**Intencionales**	Fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.
	Involuntarias	Resultantes de acciones inconscientes de usuarios, por virus electrónicos. Causadas por la falta de conocimiento en el uso de los activos.

Tabla 2.2 Tipos de amenazas

Cualquier administrador consciente de la seguridad, va a conseguir un sistema relativamente fiable de una forma lógica permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos; pero muy pocos tienen en cuenta factores como la ingeniería social. Incluso un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede causar daños sin tener acceso lógico, ni físico a los equipos, ni conocer nada sobre seguridad. Debemos estar preparados para recuperar datos perdidos o restaurar un hardware dañado.

Las amenazas más habituales provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones: Una situación no contemplada a la hora de diseñar el sistema de red o cualquier otro error, como teclear mal alguna orden, pueden comprometer local o remotamente el sistema. De este modo, cualquiera puede conseguir un exploit y dañar seriamente un sistema mediante negaciones de servicio o incluso brindando un acceso remoto, con lo que cualquier novato puede utilizarlos contra un servidor y conseguir un control total de una máquina desde su PC sin saber nada del sistema atacado.

Es de esperarse que conforme avance la tecnología también surgirán nuevas formas en las que la información puede llegar a estar expuesta, comprometiendo los principios de la seguridad de nuestra información.

2.2 Estrategias de solución en materia de seguridad de la información para las PyMEs.

La estrategia de solución para la implementación de un sistema integral de seguridad para cualquier organización, consta de cuatro fases. Ver figura 2.2.

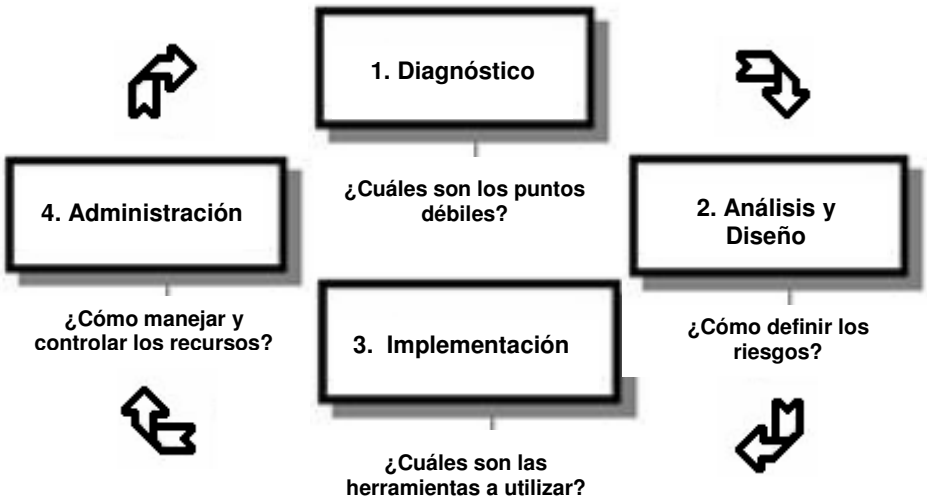


Figura 2.2 Fases para implementar un sistema de seguridad

En la tabla 2.3 podemos ver en qué consiste cada una de estas fases.

FASE	Técnica	Objetivo
FASE 1 **Diagnóstico**	Revisión de políticas (en caso de existir) y procedimientos. Revisión de la infraestructura tecnológica. Clasificación de activos. Análisis de vulnerabilidades y tests de intrusión.	Definir la situación actual de la seguridad.
FASE 2 **Análisis y Diseño**	Análisis de riesgos. Definir políticas de seguridad, planes de contingencia y/o planes de continuidad del negocio. Diseño de la arquitectura de seguridad.	Definir el plan de acción y los mejores mecanismos de seguridad a fin de minimizar los riesgos y forzar el cumplimiento de la política de seguridad.
FASE 3 **Implantación**	Implantación de procedimientos de seguridad, políticas, planes de continuidad y contingencia Implantación de la arquitectura de seguridad. Realización de pilotos / pruebas de concepto	Usar las mejores prácticas para la correcta implementación de la estrategia de seguridad.
FASE 4 **Administración**	Monitoreo y gestión de incidentes.	Integrar medidas para producir la gestión de incidentes ya sea en forma preventiva, perceptiva y/o correctiva.

Tabla 2.3 Fases para implementar un sistema de seguridad

La seguridad de la información debe ser garantizada en una forma integral y completa de ahí que resulte de mucha utilidad conocer con un poco más a detalle las estrategias de seguridad que permiten movernos desde el análisis de riesgos hasta la administración de la seguridad.

2.2.1 Fase 1: Diagnóstico

Los tres activos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar; en caso de pérdida de una aplicación, este software se puede restaurar sin problemas desde su medio original, por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación. En el caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio `original' desde el que restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad y aún así es difícil devolver los datos al estado en que se encontraban antes de la pérdida. Por tanto, la información debe ubicarse en un lugar de acceso restringido, o al menos controlado.

Debemos determinar los activos más importantes para el proceso de negocio, ya sea un servidor, una base de datos, un determinado servicio o aplicación para determinar un plan de acción a seguir para su seguridad. Identificar aquellos activos que, en caso de falla o ataque, pudieran representar grandes pérdidas para la empresa.

Identificar los procesos de negocios de la organización en que se desea implementar o analizar el nivel de seguridad de la información para así poder priorizar las acciones de seguridad en los activos que hacen parte de éstos; la relevancia de los activos en los procesos, marcará el rumbo definitivo de las acciones de seguridad, es decir, iniciar el trabajo de implementación de seguridad en las áreas más estratégicas que puedan traer un impacto mayor a la organización cuando se presente algún incidente. Dirigir los costos y optimizar los recursos donde realmente sean necesarios, delimitar los activos a ser analizados y sobre los cuales se ofrecerán las recomendaciones. Conocer los elementos constituyentes de la infraestructura de comunicación, procesamiento y almacenamiento de la información, para dimensionar dónde serán hechos los análisis y cuáles elementos serán considerados.

Para determinar la mejor solución a los requerimientos de seguridad de las PyMEs debemos entrevistarnos con las personas encargadas del área de sistemas y encontrar los procesos del negocio claves, obtener detalles sobre cómo son gestionados, implementados y utilizados, definir el nivel de capacitación necesaria del equipo involucrado, conocer la forma con que se da el flujo de información dentro del proceso y hacer un mapeo de la criticidad de estos procesos frente a las circunstancias organizacionales a que está sometido.

Para la realización de un diagnóstico completo es necesaria la realización de un test de intrusión o hackeo ético.

2.2.1.1 Test de Intrusión

Objetivos:

- Evaluar el estado de los sistemas frente a las amenazas.
- Identificar los puntos débiles para que sean corregidos y así disminuir las vulnerabilidades presentes en los activos de los procesos de negocios.

Se centra en evaluar la seguridad de los sistemas de protección perimetral de una empresa así como los diferentes sistemas que están accesibles desde Internet (routers exteriores, firewall exterior, servidores web, de correo, de noticias, etc). Intentando penetrar en ellos y de esta forma alcanzar zonas de la red de una empresa como puede ser la red interna o la DMZ. No hay una mejor forma de probar la fortaleza de los sistemas de seguridad que atacarlos. Se lleva a cabo de forma remota, quien realiza el test de penetración no tendrá información sobre la estructura de los sistemas, deberá obtenerla siguiendo las mismas pautas que un hacker intentando atacar los sistemas de la empresa y de esta forma son más objetivos. Los aspectos a revisar serán:

- *Escaneo de la Red*: Análisis para obtener un mapa detallado de la red.
- *Escaneo de puertos, identificación de servicios y sistemas operativos:* Análisis de las posibles vías de entrada a las máquinas identificando sus características y servicios. Se realiza un escaneo automático y manual (selectivo) de puertos sobre cada una de las IPs del sistema.
- *Test de vulnerabilidades:* Utilizando tanto herramientas propias como externas se determinan las deficiencias de seguridad que existen.
- *Password cracking:* Se intentan obtener cuentas de usuarios a través de herramientas automáticas o ataques por fuerza bruta, etc.
- *Document Grinding*: Recopilación de la mayor cantidad de información susceptible de ser utilizada para romper cualquiera de las protecciones.
- *Test de antivirus:* Es de vital importancia el disponer de la protección de un antivirus. Comprueba la existencia y el nivel de defensa que ofrecen.
- *Test de sistemas de confianza:* Encontrar vulnerabilidades en los sistemas analizando las relaciones de confianza o dependencias entre ellos.
- *Test de las medidas de contención:* Comprueba la existencia de herramientas de contención y el nivel de defensa que ofrecen a la llegada de código malicioso.
- *Revisión de la política de seguridad:* Se comprueba la existencia de una política que cumpla las leyes vigentes sobre seguridad de la información.
- *Test del sistema de detección de intrusos (IDS):* Análisis de los IDS con la finalidad de estudiar su reacción al recibir múltiples y variados ataques.

- *Test no Privilegiado de Aplicación:* Analizar problemas en las aplicaciones web y cookies que pudieran poner al descubierto la seguridad del sistema.
- *Test de negación de servicios:* El objetivo es saturar los servidores para que consuman todos sus recursos, con ello conoceremos el nivel de disponibilidad.

Al final se obtiene como resultado un informe detallado donde se incluye:
- Resumen ejecutivo de alto nivel.
- Detalle de todas las pruebas realizadas especificando su objetivo.
- Resultados obtenidos en las diferentes pruebas realizadas.

2.2.2 Fase 2: Análisis y Diseño

Esta fase consiste en el establecimiento de políticas de seguridad y un análisis de riesgos que bien puede ser realizado antes o después que la definición de dichas políticas. La finalidad es recolectar un conjunto de recomendaciones que permitan solucionar de la forma más acertada los problemas de seguridad encontrados; clasificarlos según su nivel de peligro y así poder elaborar un plan de acción eficiente.

2.2.2.1 Análisis De Riesgos

Objetivos:
- Encontrar las amenazas que pueden explotar las vulnerabilidades e identificar los pasos a seguir para su corrección.
- Identificar los impactos potenciales que pudieran tener los incidentes.
- Identificar la relevancia de los activos y demás recursos.

Lo primero que debe hacerse es identificar las amenazas y los recursos.

Identificación de las amenazas

Determinar una lista de amenazas que afecten a los recursos y estimar qué tan factible es que suceda cada una de ellas.

Identificación de recursos

Enlistar los recursos con los que cuente la organización. Es posible que se requiera conocer más detalladamente los procedimientos, leyes y políticas de la organización. Existen recursos tangibles (monitores, computadoras, impresoras, etc.), intangibles (privacidad de los usuarios, contraseñas de los usuarios, imagen publica, etc.)

Otros factores a considerar se muestran en la tabla 2.4

ÁMBITO	DESCRIPCIÓN	ASPECTOS POR ANALIZAR	INFORMACIÓN POR RECOPILAR
Tecnológico	El conocimiento de las configuraciones y de la disposición topológica de los activos de tecnología que componen toda la infraestructura de respaldo de la información para su almacenamiento, comunicación, procesamiento y tránsito	Los activos son de tipo aplicación y equipo, sin dejar de considerar la sensibilidad de la información que es manipulada por ellos.	Configuración: así es posible identificar la forma en que son utilizados y manipulados, buscando vulnerabilidades de seguridad Estructuras en la red de comunicación. La infraestructura que da respaldo y la forma en que es administrada por sus responsables.
Humano	Las maneras en que las personas se relacionan con los activos. Permite detectar vulnerabilidades provenientes de acciones humanas y así es posible dirigir recomendaciones para garantizar la continuidad de los negocios de la organización.	Los usuarios, tanto los que respaldan y utilizan como los administradores, deben mostrar el grado de conciencia en relación al nivel de la información que manejan. Evaluar hasta qué punto los involucrados son conscientes de la seguridad necesaria.	El nivel de acceso que las personas tienen en la red o en las aplicaciones. Las restricciones y permisos que deben tener para realizar sus tareas. El nivel de capacitación y formación educativa que necesitan para tener acceso y para manipularlos, etc.
Procesos	Análisis de flujo de información y de cómo son administrados los recursos. Identificar los eslabones entre las actividades y los insumos necesarios para su realización con el objetivo de identificar las vulnerabilidades que puedan afectar la seguridad.	Identificar las personas involucradas en el flujo de información, evaluar la necesidad real de acceso que ellas tienen a los activos. Evaluar el impacto del uso indebido de la información por personas no calificadas.	Identificar la relevancia de los activos determinantes para el proceso de negocio. Cada activo debe ser considerado en una escala de valor crítico, determinar qué tan importante es para nuestro negocio en comparación con el resto de los activos de la empresa, para priorizar las acciones de corrección y protección.
Físico	Identificar en la infraestructura física los activos que tengan vulnerabilidades que puedan traer algún perjuicio a la información y a los demás activos. Evaluar el impacto de accesos indebidos a las áreas en donde se encuentran activos tecnológicos. Evaluar el impacto de desastres naturales. Identificar fallas en la localización física de los activos tecnológicos.	Visita técnica en los entornos donde se realizan actividades relacionadas directa o indirectamente con los procesos de negocio que están siendo analizados, a los cuales se deben atribuir soluciones de seguridad.	Disposición organizativa del espacio: ver como están acomodados los muebles y los activos. Que las áreas de circulación de personas estén libres de activos de valor o importancia. Sistemas de combate a incendio: Que estén en los lugares adecuados: detectores de humo, extintores, entre otras cosas. Control de acceso: Sistemas de detección y autorización de acceso a las de personas: cámaras de video, personal de vigilancia, trinquete para acceso, biométricos, entre otros.

Tabla 2.4 Ámbitos a considerar en un análisis de riesgos

Una vez que se tomaron en cuenta estos factores, se inician las acciones de distribución de ellas para reducir los riesgos a que está sometida la infraestructura que respalda uno o más procesos de negocio.

Para la realización del análisis de riesgos es importante considerar la relación costo-beneficio. Este cálculo permite que sean evaluadas las medidas de seguridad con relación a su aplicabilidad y el beneficio que se agregará al negocio. Tras obtener mediante cualquier mecanismo los indicadores de riesgo llega la hora de evaluarlos para tomar decisiones acerca de la gestión de nuestra seguridad y sus prioridades.

El **riesgo calculado** son los costos de pérdida que pueden ser bastante difíciles de averiguar puesto que muchas veces se trata con beneficios intangibles. Se debe establecer cuáles son los costos de no disponibilidad de un servicio por un determinado tiempo, daño parcial del servicio o pérdida permanente.

Este riesgo calculado se comparará con un cierto **umbral de riesgo** que puede ser un número, por ejemplo, podemos asignar un valor de 0 a 10, donde 10 implica más probabilidad de riesgo; o bien una etiqueta de riesgo: nivel de amenaza alto, impacto alto, vulnerabilidad grave, etc.

Si el riesgo calculado es superior al umbral implica una decisión de reducción de riesgo. Si por el contrario el calculado es menor que el umbral, se habla de **riesgo residual**, y se considera **riesgo asumido**, es decir, no hay porqué tomar medidas para reducirlo. Se trata de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que nos costaría recuperarnos de un daño en él o de su pérdida total.

De esta forma podemos listar cada recurso con su nombre y el número o etiqueta asignado. Evidentemente, los recursos que presenten un riesgo mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. Es especialmente importante un grupo de riesgos denominados **inaceptables**, aquellos cuyo peso supera un cierto umbral; se trata de problemas que no nos podemos permitir en nuestros sistemas, por lo que su prevención es crucial para que todo funcione correctamente.

El costo de prevención es fácil de obtener si conocemos las posibles medidas de prevención que tenemos a nuestra disposición: por ejemplo, para saber lo que nos cuesta prevenir los efectos de un incendio en la sala de operaciones, no tenemos más que consultar los precios de sistemas de extinción de fuego, o para saber lo que nos cuesta proteger nuestra red sólo hemos de ver los precios de productos como firewall o detectores de intrusos que bloqueen paquetes.

No sólo hemos de tener en cuenta el costo de cierto mecanismo, sino también lo que nos puede suponer su implementación y su mantenimiento; en muchos

casos existen soluciones gratuitas para prevenir ciertas amenazas, pero estas soluciones tienen un costo asociado relativo a la dificultad de hacerlas funcionar correctamente, por ejemplo dedicando a un empleado o un equipo para su administración y monitoreo.

Si en una empresa existen áreas que son comúnmente atacadas y afectadas, es posible que sea necesario atender primero estos procesos dado los riesgos que pudieran presentar para la seguridad de la información en la empresa. O bien, si en la empresa existen áreas que son importantes para la reducción de costos, pudiera ser importante considerarlas como clave y de alta prioridad para las acciones de seguridad por tomar. Ver Tabla 2.5.

FACTOR	ACCIÖN
Alta prioridad, procesos críticos para el negocio y activos afectados anteriormente (Información Secreta)	Implementación inmediata de mecanismos de seguridad
Información sensitiva y/o restringida	Medidas correctivas y/o preventivas en corto tiempo
Información de bajo riesgo (Información pública)	Aumentar margen de tiempo en el plan de acción.

Tabla 2.5 Factores a considerar para priorizar los activos

Hemos de tener siempre presente que los riesgos se pueden minimizar, pero nunca eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención ante un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas proactivas, siendo aquellas que se toman para prevenir un problema, y medidas reactivas, una vez que el daño se produce, son las que se ponen en práctica para minimizar sus efectos.

Una vez que se realiza el análisis de riesgos, la organización tiene en sus manos una poderosa herramienta para el tratamiento de sus vulnerabilidades y un diagnóstico general sobre el estado de la seguridad. A partir de este momento es posible establecer políticas para la corrección de los problemas ya detectados, y la gestión de seguridad de ellos a lo largo del tiempo, para garantizar que las vulnerabilidades encontradas sean gestionadas.

El análisis de riesgos tiene como resultado los informes de recomendaciones de seguridad, para que la organización pueda evaluar los riesgos a que está sometida y conocer cuáles son los activos de los procesos de negocio que están más susceptibles a la acción de amenazas a la CIA de la información.

El análisis de riesgos puede ocurrir antes o después de la definición de una política de seguridad. Según la norma internacional BS/ISO/IEC 17799, esta actividad puede ser hecha después de la definición de la política.

El análisis de riesgos no debe ser hecho una sola vez y olvidado, debe ser actualizado periódicamente.

2.2.2.2 Políticas de Seguridad

Objetivos:

- Permiten la identificación y control de amenazas y puntos débiles
- Estandardizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico.
- Determinar la amplitud que tendrá en relación a entornos, individuos, áreas y departamentos.
- Establecer las relaciones de responsabilidad para el cumplimiento de tareas así como la aplicación de sanciones resultantes de casos de inconformidad con la política elaborada.

Tras identificar todos los recursos que deseamos proteger, así como las posibles vulnerabilidades y amenazas a que nos exponemos, hemos de estudiar cómo proteger nuestros sistemas, sin ofrecer aún implementaciones concretas para protegerlos ya que apenas se establecerán las políticas, más adelante se determinarán los mecanismos necesarios para su implementación.

Debemos indicar qué se va a permitir y qué se va a denegar. Para esto existen dos paradigmas de seguridad; el sentido de redacción y elaboración del manual de políticas se puede suscribir en cualquiera de los dos términos.

- *Política Restrictiva*.- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos.
- *Política Permisiva*.- Se permite cualquier servicio excepto aquellos expresamente prohibidos.

La forma más recomendada y utilizada es la correspondiente a la elaboración de políticas restrictivas, y aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a algún servicio, las razones de esta decisión quedan debidamente asentadas y justificadas en el mismo manual de políticas de seguridad informática para la organización en cuestión.

La política al ser utilizada de manera correcta, brinda ventajas como lo son:

1. Definir controles en sistemas informáticos.
2. Establecer los derechos de acceso con base en las funciones de cada persona.
3. Orientación de los usuarios con relación a la disciplina necesaria para evitar violaciones de seguridad.
4. Establece exigencias que pretenden evitar que la organización sea perjudicada en casos de fallos de seguridad.
5. Permite la realización de investigaciones de delitos por computadora.

Es una medida que busca establecer los estándares de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos. Es una forma de suministrar un conjunto de normas internas para guiar la acción de las personas en la realización de sus trabajos y aumentar el nivel de seguridad y compromiso de cada uno de los involucrados, pues está orientada hacia la

formación de hábitos, por medio de manuales de instrucción y procedimientos operativos.

A partir de las políticas de seguridad, es posible hacer de la seguridad de la información un esfuerzo común, en tanto que todos puedan contar con información documentada y normalizada. Debido a que una política de seguridad impacta la forma de trabajo diario de las personas, ésta debe ser:

- Clara, escrita en buena forma y lenguaje no elevado,
- Concisa, evitar información innecesaria o redundante,
- Acorde con la realidad práctica de la empresa,
- Actualizada periódicamente.

La política debe ser elaborada tomando como base la cultura de la organización y el conocimiento especializado de seguridad de los profesionales involucrados con su aplicación. Se debe formar un equipo multidisciplinario que represente gran parte de los aspectos culturales y técnicos de la organización. Identificar junto a los usuarios y administradores las preocupaciones que ellos tienen con los activos, los procesos de negocio, áreas o tareas que ejecutan o en la cual participan. Debe contener también la asignación de responsabilidades de las personas involucradas donde queden claros los roles de cada uno.

Como la información no está presente únicamente en medios electrónicos sino también en fax, papel, comunicación de voz, etc., la política debe permitir que se aplique a cualquier ambiente existente y no contener términos técnicos de informática. Debe tratarse de un texto, no técnico, con las reglas generales que guían a la elaboración de las normas de seguridad.

Dentro de la política de seguridad es necesario considerar elementos que determinen las bases mínimas a seguir en materia de configuración y administración de la tecnología. Por ejemplo, establecer que los servidores con información crítica de la empresa no deben prestar servicio de estaciones de trabajo a los empleados.

Durante su elaboración no podemos olvidar el lado humano, los descuidos, falta de capacitación, interés, etc. Deberá hacerse oficial la política una vez que se tenga definida, esto dará por entendido la aprobación por parte de la administración de la empresa. Debe ser publicada y comunicada de manera adecuada para todos los empleados, socios, terceros y clientes.

Elaborar una política es un proceso que exige tiempo e información. Toda documentación ya existente debe ser analizada con relación a los principios de seguridad de la información, para aprovechar al máximo las prácticas actuales, evaluar y agregar seguridad a esas tareas. Entre la documentación existente, se pueden considerar: manuales operativos y de mejores prácticas, metodologías, políticas de calidad y otras.

Es importante aclarar cualquier duda conceptual que pueda surgir en el momento de la lectura de la política. Así todos los lectores deben tener el mismo punto de referencia conceptual de términos. Por lo tanto se recomienda que la política cuente con un glosario específico donde se especifiquen los términos y conceptos presentes en toda la política de seguridad.

Los temas a tratar en una política de seguridad son:

- *Seguridad física*: acceso físico, infraestructura del edificio, centro de datos.
- *Seguridad de la red corporativa:* configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.
- *Seguridad de usuarios*: uso de contraseñas complejas, seguridad en estaciones de trabajo, formación y creación de conciencia.
- *Seguridad de datos*: criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.
- *Auditoría de seguridad*: análisis de riesgos, revisiones periódicas, visitas técnicas, monitoreo y auditoría.
- *Aspectos legales*: contratos y acuerdos comerciales, leyes y reglamentación gubernamental.

Las partes principales con que debe contar toda política son:

Directrices (Estrategias)

Conjunto de reglas generales de nivel estratégico donde se expresan los valores de seguridad de la organización.

Corresponden a las preocupaciones de la empresa sobre la seguridad de la información, al establecer sus objetivos, medios y responsabilidades.

Los valores que deben ser seguidos, para que el principal patrimonio de la empresa, que es la información, tenga el nivel de seguridad exigido.

Normas (Táctico)

Conjunto de reglas generales y específicas de la seguridad de la información que deben ser usadas por todos los segmentos involucrados en los procesos de negocio de la institución, y que pueden ser elaboradas por activo, área, tecnología, proceso de negocio, público a que se destina, etc.

Las normas, por estar en un nivel táctico, pueden ser específicas para el público a que se destina, por ejemplo para técnicos y para usuarios.

- *Normas de Seguridad para técnicos*: Reglas generales de seguridad de información dirigida para quien cuida de ambientes informatizados (administradores de red, técnicos etc.), basadas en los aspectos más genéricos como periodicidad para cambio de contraseñas, copias de seguridad, acceso físico y otros. Pueden ser ampliamente utilizadas para la configuración y administración de ambientes diversos.
- *Normas de Seguridad para Usuarios*: Reglas generales de seguridad de la información dirigidas para hacer uso de ambientes informatizados,

basadas en aspectos más genéricos como cuidados de contraseñas, cuidados con los equipos, cuentas de usuarios, y otros.

Procedimiento (Operacional)

Conjunto de orientaciones para realizar las actividades operativas de seguridad, que representa las relaciones interpersonales e ínter departamentales y sus respectivas etapas de trabajo para la implantación o manutención de la seguridad de la información.

Instrucción de trabajo (Operacional)

Conjunto de comandos operativos a ser ejecutados en el momento de la realización de un procedimiento de seguridad establecido en modelo de paso a paso para los usuarios del activo en cuestión.

Una política debe tener como base una estrategia de medición de eficacia, para poder evaluar el desempeño de la gestión de seguridad y los puntos débiles que necesitan ser mejorados.

En caso de realizar el análisis de riesgos habiendo sido ya establecidas las políticas, éstas nos permiten delimitar el alcance del análisis, ser selectivos en la verificación de activos que la política establece como vulnerables. El análisis tomará en cuenta la lista de amenazas potenciales que la misma política contempla.

2.2.2.3 Mecanismos de seguridad

Después de conocer las amenazas y puntos débiles del ambiente, adquiridos en el análisis de riesgos, o después de la definición formal de la política de seguridad de la información, debemos tomar algunas medidas para la implementación de las acciones de seguridad recomendadas o establecidas.

Los mecanismos utilizados para forzar el cumplimiento de la política de seguridad que se definió se les denomina mecanismos de seguridad; son la parte más visible de nuestro sistema de seguridad, y se convierten en las medidas básicas para garantizar la protección de los sistemas de información.

Sus acciones deben ser orientadas hacia la eliminación de vulnerabilidades, teniendo como objetivo evitar que una amenaza se vuelva realidad. Estas medidas son el paso inicial para el aumento de la seguridad de la información en un ambiente TI.

Podemos ver los diferentes tipos de mecanismos en la tabla 2.6.

Mecanismo	Descripción	Ejemplos
Preventivos	Buscando evitar el surgimiento de nuevos puntos débiles y amenazas. Por ejemplo, antivirus, actualización automática de parches de seguridad del sistema operativo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde una red.	**Protección contra virus** Implementación de un software que prevenga y detecte software maliciosos, para minimizar los riesgos de fallos en el sistema o la pérdida de información. **Autenticación e identificación** Identifican entidades del sistema de una forma única, y una vez identificadas, autenticarlas, comprobar que la entidad es quién dice ser. Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto. **Control de acceso** Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema. *Control de acceso a los recursos de la red:* Implementación de controles en las estaciones de trabajo y configuración de seguridad en los servidores, para garantizar un control mayor en el uso de servicios y recursos disponibles. *Seguridad para equipos portátiles:* Implantación de aplicaciones y dispositivos para la prevención contra accesos indebidos y el robo de información. *Seguridad para las aplicaciones:* Implementación de dispositivos y aplicaciones para garantizar la confidencialidad, y el control del acceso, además del análisis de las vulnerabilidades de la aplicación, al suministrar una serie de recomendaciones y estándares de seguridad. **Mecanismos de separación** Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso. **Mecanismos de seguridad en las comunicaciones** Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Cada vez se utilizan más los protocolos seguros, aún es frecuente encontrar conexiones en texto claro ya no sólo entre máquinas de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red. Para garantizar esta seguridad en las comunicaciones, hemos de utilizar ciertos mecanismos, como: *Infraestructura de llaves públicas y privadas:* Consiste en emplear servicios, protocolos y aplicaciones para la gestión de claves públicas, que suministren servicios de criptografía y firma digital. *Virtual private network (VPN):* Hace factible la comunicación segura y de bajo costo. Utiliza una red pública, como Internet, para enlazar dos o más puntos, y permite el intercambio de información empleando criptografía. *Acceso remoto seguro:* Hace posible el acceso a los recursos de la red al emplear una red pública, como Internet.

Tabla 2.6 Mecanismos de seguridad

Mecanismo	Descripción	Ejemplos
Perceptivos o detección	Orientado hacia la revelación de actos que pongan en riesgo la información, como el detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los detectores de intrusos, firewall y sistemas de filtrado de contenido, etc.	**Firewall** Sistema que controla el tránsito entre dos o más redes, permite el aislamiento de diferentes perímetros de seguridad, como por ejemplo, la red Interna e Internet. En algunos casos puede existir un firewall interno que funciona al aislar el acceso a la red de servidores críticos, minimizando los riesgos de invasiones internas a servidores y aplicaciones de misión crítica. **Sistema de detección de intrusos (IDS)** Implantación de una herramienta que analice el tránsito de la red en busca de posibles ataques, para permitir dar respuestas en tiempo real, y reducir así los riesgos de invasiones en el sistema. **Seguridad en correo electrónico** Utiliza certificados digitales para garantizar el sigilo de las informaciones y software para filtro de contenido, y proteger a la empresa de aplicaciones maliciosas que llegan por ese medio.
Correctivos o de recuperación	La reparación de los problemas de seguridad conforme su ocurrencia. Se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional.	**Mecanismos de análisis forense** Su objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación a la seguridad, las actividades que realizó el intruso y la forma utilizada para entrar en el sistema; de esta forma se previenen ataques posteriores y detectan posibles vulnerabilidades a otros sistemas de nuestra red. **Plan de contingencia** Es el conjunto de procedimientos de resolución y procesos alternativos que ha de realizar una organización cuando ocurre una interrupción por culpa de un incidente de fuerza mayor en los procesos de negocio habituales. **Plan de continuidad** Un plan de continuidad de negocio consiste en un análisis de las áreas que servirá para establecer una política de recuperación ante un desastre. Tiene como objetivo tratar de alcanzar una máxima disponibilidad para la infraestructura crítica. Debemos determinar cuáles son los recursos de información relacionados con los procesos críticos del negocio de la organización y cuál es el período de tiempo de recuperación crítico para los recursos de información en el cual se debe establecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o aceptables.

Tabla 2.6 Mecanismos de seguridad (continuación)

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad de nuestro sistema, hemos de enfatizar en el uso de mecanismos de prevención y de detección; evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar a su estado original tras un incidente. Si lográramos un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención y detección de una forma completa, no necesitaríamos mecanismos de recuperación. Por supuesto, en la práctica no existe tal sistema.

Un plan de continuidad, a diferencia de uno de contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado. Mientras que el plan de contingencia se concentra en la recuperación de eventos únicos que producen una interrupción prolongada del servicio, el plan de continuidad se ejecuta permanentemente a través de la administración de riesgos tanto en la información como en la operación. El enfoque del plan de contingencia se basa en la minimización del impacto que pueda tener un desastre en la compañía, mientras que el plan de continuidad está orientado a asegurar la satisfacción del cliente, la prestación de los servicios y el correcto uso de los recursos de la red, para mantenerla productividad a pesar de una catástrofe. El plan de continuidad es costoso y no es para todas las empresas, requiere un adecuado estudio de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, pues para algunas empresas se deberá contar con un plan de continuidad, para otros, bastará con un plan de contingencia.

2.2.2.4 Arquitectura de seguridad

Al conjunto de mecanismos implementados se le denomina arquitectura de seguridad. Desde el punto de vista de soluciones tecnológicas, una arquitectura de seguridad lógica debe conformarse al menos por: software antivirus, soluciones de autentificación, firewall e IDS. Claro que ésta deberá incrementarse o disminuirse dependiendo de los niveles de seguridad requeridos.

En lo referente a los antivirus, sabemos que son herramientas de seguridad básicas para cualquier computadora personal; sin embargo, en el caso de las empresas, conviene colocar un servidor de antivirus, como parte del sistema de seguridad perimetral. En este trabajo tan solo mencionaremos la importancia de instalarlo y mantenerlo al día en cuanto actualizaciones y firmas, así mismo, es responsabilidad del administrador de seguridad estar en listas de noticias referentes a las nuevas amenazas para tomar las medidas necesarias para su prevención.

Como hemos dicho, nuestra arquitectura ha de incluir al menos un sistema que permita identificar a las entidades, generalmente usuarios, que intentan acceder a los objetos, por ejemplo, bases de datos; mediante procesos tan simples como una contraseña o tan complejos como un dispositivo biométrico.

Se suelen dividir en tres grandes categorías en función de lo que utilizan para la verificación de identidad. Por supuesto, un sistema de autenticación puede combinar mecanismos de diferente tipo, y así incrementar su fiabilidad como es el caso de una tarjeta de crédito junto al PIN a la hora de utilizar un cajero automático.

2.2.2.5 Mecanismos de autenticación

Sistemas basados en algo conocido: contraseñas

Evidentemente, es la más vulnerable a todo tipo de ataques, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior. Ambas acuerdan una clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, y si ésta es correcta se otorga el acceso a un recurso o sistema.

Sistemas basados en algo poseído: tarjetas inteligentes

Es un dispositivo de seguridad resistente a la adulteración, que ofrece funciones para un almacenamiento y procesamiento seguro de información. Poseen un chip empotrado que puede implementar un sistema de ficheros cifrado y funciones criptográficas, y además puede detectar activamente intentos no válidos de acceso a la información almacenada; este chip inteligente es lo que las diferencia de las simples tarjetas de crédito, que solamente incorporan una banda magnética donde va almacenada cierta información del propietario de la tarjeta.

Se necesita introducir la tarjeta en un hardware lector; los dos dispositivos se identifican entre sí con un protocolo a dos bandas en el que es necesario que ambos conozcan la misma clave, lo que elimina la posibilidad de utilizar otras tarjetas para autenticarse ante determinado lector.

Las ventajas son muchas frente a las desventajas; se trata de un modelo ampliamente aceptado entre los usuarios; es rápido e incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Además, su uso es factible tanto para controles de acceso físico como para controles de acceso lógico. Se integra fácilmente con otros mecanismos de autenticación como las contraseñas; y en caso de desear

bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuando la introduzca en el lector o marcarla como inválida en una base de datos, por ejemplo, si se equivoca varias veces al teclear su PIN, igual que sucede con una tarjeta de crédito normal.

Como principal inconveniente podemos citar el costo que supone para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas; aparte, que un usuario pierda su tarjeta es bastante fácil, y durante el tiempo que no disponga de ella o no puede acceder al sistema, o hemos de establecer reglas especiales que pueden comprometer nuestra seguridad.

Mecanismos de autenticación biométricos

Basados en una característica física del usuario, ejemplo la huella dactilar; o un acto involuntario del mismo, como es la firma ya que no se piensa en el diseño de cada trazo individualmente. La criptología se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones retinales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos.

Inclusive parece que en un futuro no muy lejano estos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para el usuario ya no va a necesitar recordar contraseñas o números de identificación complejos, y, no habrá el problema de que olvidó su tarjeta de identificación en casa. Son sistemas mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento.

Las características básicas de fiabilidad de los sistemas de autenticación son:

- *Tasa de falso rechazo*.- Probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente,
- *Tasa de falsa aceptación*.- Probabilidad de que autentique correctamente a un usuario ilegítimo

Evidentemente, una alta tasa de falso rechazo provoca descontento entre los usuarios del sistema, pero una elevada tasa de falsa aceptación genera un grave problema de seguridad.

Los mecanismos de seguridad empleados en nuestra arquitectura deben ser adecuados a la información que se intenta proteger, si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto.

A continuación hablaremos del elemento más popular a la hora de hablar de seguridad, aunque dista mucho de ser la solución final a los problemas.

2.2.2.6 Firewall

Es un sistema que hace cumplir una política de control de acceso entre dos redes, una de confianza y una red de seguridad desconocida, es utilizado para asegurar una máquina o subred, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él; sólo el tráfico autorizado, definido por la política de seguridad, es permitido.

La implementación de un firewall es esencial para nuestra arquitectura de seguridad; sin embargo, así como presenta diversas ventajas también tiene sus inconvenientes como podemos apreciar en la tabla 2.7

Beneficios	Limitaciones
▪ Refuerzan la política de seguridad. ▪ Restringen el acceso a servicios específicos. ▪ Proporcionan una excelente herramienta de auditoría ▪ Es el punto ideal para monitorear la seguridad de la red ▪ Genera alarmas de intentos de ataque al responsable. ▪ Brinda estadísticas del ancho de banda utilizado y los procesos que han influido más en el tráfico de la red; así, el administrador puede restringir o aprovechar mejor el ancho de banda disponible.	▪ No ofrecen protección ante lo que esta autorizado. ▪ No defiende de la ingeniería social o de un usuario autorizado con propósitos maliciosos. ▪ No son sistemas inteligentes, actúan de acuerdo a parámetros introducidos, si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. ▪ No provee de herramientas contra la filtración de software o archivos infectados con virus.

Tabla 2.7. Ventajas y desventajas del Firewall.

Evidentemente la forma más efectiva de proteger nuestra red consiste en el aislamiento físico, es decir, no tener conectada la máquina o la subred a otros equipos o a Internet. Ver Figura 2.3.

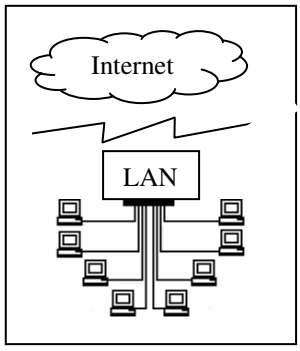


Figura 2.3: Aislamiento.

Sin embargo, la mayoría de organizaciones necesitan compartir información por lo que no es posible un aislamiento total. El punto opuesto consistiría en una conectividad completa con la red, lo que desde el punto de vista de la seguridad es muy problemático: cualquiera, desde cualquier parte del mundo, puede

potencialmente tener acceso a nuestros recursos y con ello a una serie de privilegios. Ver Figura 2.4

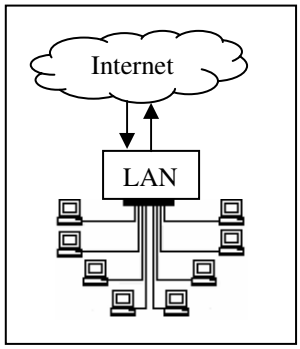


Figura 2.4: Conexión total.

Un término medio consiste en implementar cierta separación lógica mediante un firewall. Obteniendo así un espacio protegido, denominado **perímetro de seguridad**, y una red externa, no confiable, llamada **zona de riesgo**. Figura 2.5

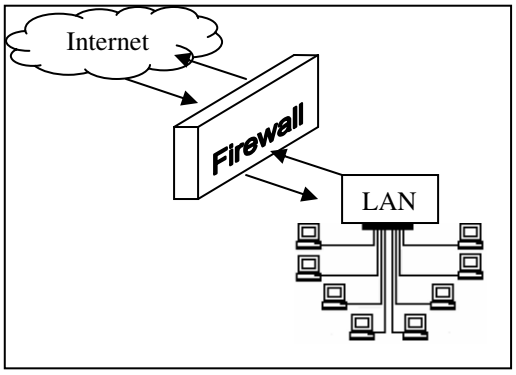


Figura 2.5: Firewall entre la zona de riesgo y el perímetro de seguridad.

Diseños habituales de firewall

El perímetro de red puede diseñarse utilizando diversas técnicas para proporcionar niveles de seguridad, acceso y rendimiento.

Zona Desmilitarizada (DMZ)
Añade un nivel de seguridad en las arquitecturas de firewall situando una subred entre las redes externa e interna, no existe una conexión directa entre éstas, de forma que se consiguen reducir los efectos de un ataque de un intruso que acceda y de este modo no consiga un acceso total a la red interna protegida. La DMZ aísla físicamente los servicios internos, separándolos de los servicios públicos.

Host Bastion
Es un sistema especialmente asegurado, pero vulnerable a todo tipo de ataques por estar abierto a Internet; es el punto de contacto de los usuarios de la red interna con otro tipo de redes. Esconde la configuración de la red hacia el exterior.

Puerta de enlace de filtrado (choke point)
Se hace pasar todo el tráfico de la red por un solo punto y filtra tráfico de entrada y salida. Puede ser el mismo host bastión o un elemento diferente, como un router. Realiza un filtrado de paquetes denegando o permitiendo el flujo de tramas entre dos redes, de acuerdo a unas reglas predefinidas.

Puede haber firewalls con un choke point y un host bastión, aunque también se considera firewall a un simple router filtrando paquetes, es decir, actuando como choke point. Los router son la primera capa de protección en una arquitectura de seguridad general, y a veces, se utilizan en lugar de un firewall, sobre todo en redes pequeñas, ya que éstas no pueden costearse un dispositivo independiente y la asistencia técnica que requiere.

Tecnologías de Firewall

Actualmente existen cuatro categorías principales:

1. Filtrado de Paquetes (Packet Filter)
2. Puestas de enlace de aplicación (Proxy – Gateway de Aplicación)
3. Puertas de enlace de nivel de circuito (Circuit Level Gateway)
4. Inspección de paquetes con estado (Stateful Packet Inspection, SPI)

Si desea mayor información sobre el funcionamiento de cada uno de estos puede ver el apéndice A. No se puede considerar que un tipo de firewall sea mejor que otro ya que cada uno posee funciones específicas. La combinación de éstas ofrece el mayor nivel de seguridad posible y es recomendable.

Es importante recordar que los productos de firewall existentes hoy en día suelen combinar dos o más tipos de firewall en un solo producto. El utilizar un solo producto que combina diferentes tipos tiene el inconveniente de generar un punto único de fallo pero es aceptable para la mayoría de las configuraciones.

Algunos firewalls permiten el acceso selectivo de determinados usuarios externos a ciertos servicios o deniegan cualquier tipo de acceso a otros, a esto se le llama niveles de confianza.

- *Usuarios internos con permiso de salida para servicios restringidos.*- Permite especificar una serie de redes y direcciones a los que denomina Trusted (validados)**.** Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
- *Usuarios externos con permiso de entrada desde el exterior.*- Este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna. Lo más conveniente es que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

Los firewall son cada vez más necesarios en nuestras redes, pero todos los expertos recomiendan que no se usen en lugar de otras herramientas, sino junto a ellas; el firewall trabaja mejor si se complementa con una defensa interna ya que no protegen contra ataques que no pasan por él, sólo sirve de defensa perimetral de las redes, no defiende de ataques o errores provenientes del interior. 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 modem en sus PCs o estaciones de trabajo; esto, tan habitual en muchas organizaciones, supone la violación y la ruptura total del perímetro de seguridad, ya que posibilita accesos a la red no controlados por el firewall.

Generalmente un administrador que disponga de un firewall asume que toda su red es segura, por lo que suele descuidar enormemente la seguridad de los equipos de la red interna. Los firewalls no ofrecen protección una vez que el intruso lo traspasa, de forma que si éste se ve comprometido y el resto de nuestra red no está lo suficientemente protegida el atacante consigue amenazar a toda la subred. Otro problema es la reconfiguración de los sistemas al pasarlos de una zona a otra con diferente nivel de seguridad; este acto, que en ocasiones no implica ni 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.

2.2.2.7 Sistemas detectores de intrusos (IDS, Intrusion Detection Systems)

A pesar de que un enfoque clásico de la seguridad de un sistema informático siempre define como principal defensa del mismo sus controles de acceso en un firewall, esta visión es extremadamente simplista si no tenemos en cuenta que en muchos casos esos controles no pueden protegernos ante un ataque. Por ejemplo, pensemos en un firewall donde hemos implantado una política que deje acceder al puerto 80 de nuestros servidores web desde cualquier máquina de Internet; esto sólo comprobará si el puerto destino de una trama es el que hemos decidido para el servicio HTTP, pero seguramente no tendrá en cuenta si ese tráfico representa o no un ataque o una violación de nuestra política de seguridad; no detendrá a un atacante que trate de acceder al archivo de contraseñas de una máquina aprovechando un bug del servidor web. Nuestro entorno de trabajo no va a estar nunca a salvo de intrusiones ya sea un hacker o un usuario autorizado que intenta obtener privilegios que no le corresponden.

Los sistemas utilizados para detectar las intrusiones o intentos de intrusión se les denomina sistemas de detección de intrusos (Intrusion Detection Systems, IDS). Además del sistema de protección perimetral basado en firewall, debe colocarse un IDS entre el firewall y la red interna, además cada sistema habrá de estar configurado de una manera correcta, de forma que incluso si el firewall

falla cualquier máquina pudiera seguirse considerando relativamente segura; hemos de ser capaces de detectar cualquier anomalía tan pronto como sea posible, incluso antes de que se produzca. Aunque nuestras políticas de seguridad no fueran violadas, los sistemas de detección de intrusos se encargarán de mostrarnos todos los intentos de penetrar en nuestro entorno.

Clasificación de los IDS

Existen dos maneras de clasificar los IDS, la primera de ellas es en función de qué sistemas vigilan.

IDS basados en red

Monitorea los paquetes que circulan por nuestra red, en un mismo dominio de colisión, en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico, como un switch o un router.

IDS basados en máquina

Realizan su función protegiendo un único sistema; es un proceso que trabaja periódicamente buscando patrones que puedan denotar un intento de intrusión y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado. Existen tres subcategorías:

- *Verificadores de integridad del sistema (SIV).-* Mecanismo encargado de monitorear una máquina en busca de posibles modificaciones no autorizadas, como serían las backdoors dejadas por un intruso
- *Monitores de registros (LFM).-* Monitorean los logs generados por los programas de una máquina en busca de patrones que puedan indicar un ataque o una intrusión.
- *Sistemas de decepción.-* También conocidos como tarros de miel (honeypots), son mecanismos encargados de simular servicios con fallas de seguridad de forma que un hacker piense que realmente se puede acceder a un sistema, cuando en realidad se está aprovechando para registrar todas sus actividades y saber que tipos de exploits utiliza.

Esta división queda algo pobre, ya que cada día se avanza más en la construcción de sistemas de detección de intrusos basados en host que no podrían englobarse en ninguna de las subcategorías anteriores.

Otra clasificación de los IDS se realiza en función de cómo actúan:

Detección de anomalías

La base de su funcionamiento es suponer que una intrusión se puede ver como una anomalía de nuestro sistema, por lo que si somos capaces de establecer un perfil del comportamiento habitual de los sistemas seremos capaces de detectar las intrusiones por pura estadística: una intrusión sería una desviación excesiva de la media de nuestro perfil de comportamiento.

Detección de usos indebidos

Presupone que podemos establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones; mientras que la detección de anomalías conoce lo normal y detecta lo que no lo es, este esquema se limita a conocer lo anormal para poderlo detectar.

Existen IDS de tiempo real (Real-Time Intrusion Detection Systems) que trabajan continuamente en busca de posibles ataques y también hay sistemas, analizadores de vulnerabilidades (Vulnerability Scanners), que se ejecutan a intervalos, el administrador ha de ejecutarlos regularmente, ya sea de forma manual o automática, contra sus sistemas para verificar que no presentan problemas de seguridad.

Requisitos de un IDS

- *Ejecución continua.-* Independientemente de que al detectar un problema se informe a un operador o se lance una respuesta automática, el funcionamiento habitual no debe implicar interacción con un humano. Deben ser mecanismos automatizados que se instalan y configuran de forma que su trabajo habitual sea transparente a los operadores del entorno informático.
- *Aceptabilidad.-* No generar una cantidad elevada de falsos positivos (detección de intrusiones que realmente no lo son) o de logs, ya que entonces llegará un momento en que nadie se preocupe de comprobar las alertas emitidas por el detector.
- *Adaptabilidad a cambios en el entorno de trabajo.-* Ningún sistema informático puede considerarse estático; todo cambia con una periodicidad más o menos elevada. Si nuestros mecanismos de detección de intrusos no son capaces de adaptarse rápidamente a esos cambios, están condenados al fracaso.
- *Tolerancia a fallos o capacidad de respuesta ante situaciones inesperadas.-* Por ejemplo, un reinicio inesperado de varias máquinas o un intento de engaño hacia el IDS.

2.2.2.8 Redes Privadas virtuales (VPN, Virtual Private Network)

Las organizaciones que cuentan con oficinas remotas o requieren de acceso a terceros necesitan conexiones que cumplan con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

La VPN es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Una VPN es una red privada que se extiende, mediante un proceso de encapsulamiento y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública dedicado únicamente para nuestros datos para que estos viajen con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto. Ver figura 2.6

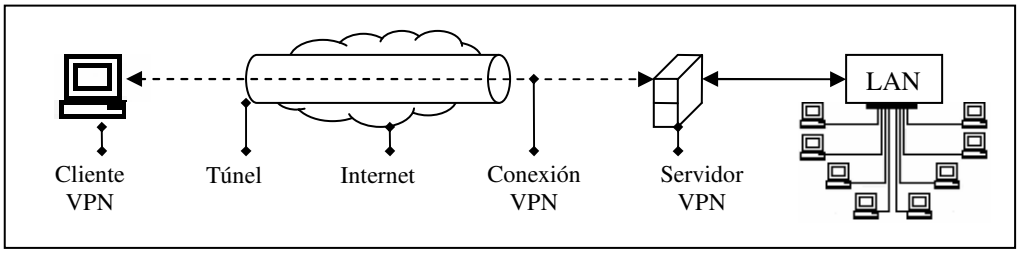


Figura 2.6 Diagrama de VPN

Los costos son bajos y brindan la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad. Tienen cada vez más aceptación en las redes actuales. Proporcionan un método para crear una conexión virtual segura entre diferentes sitios, que funciona de forma parecida a una conexión física punto a punto. El transporte se realiza a través de una infraestructura WAN. Los dispositivos que se encuentran a lo largo de la ruta VPN no pueden insertar o ver el tráfico que se transmite por la VPN.

Una vez diseñadas las implementaciones VPN se deberá considerar la ruta física para asegurarse de que dispone de ancho de banda suficiente y fiable para controlar el tráfico esperado a través de la ruta real y cualquier VPN implantada sobre el mismo.

Los dos extremos de una VPN se denotan principales y estos deben estar de acuerdo sobre los protocolos, filtros de tráfico y el material para crear claves y poder mantener una conexión segura. Los principales pueden ser diversos dispositivos de red como un firewall, un router o un equipo de host.

Al igual que las conexiones físicas WAN, los vínculos VPN amplían el perímetro de seguridad. Debe asegurarse que la WAN este bien protegida. Cuando los sitios de confianza se conectan mediante VPN a través de un firewall, la red es tan segura como la directiva más débil del firewall.

Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas

empresas han reemplazado con esta tecnología su infraestructura *dial-up* (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos modems.

VPN punto a punto (site to site)

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, también llamada tecnología de túnel o tunneling.

Tunneling

Esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura, en este caso de ssh, el túnel por el cual enviamos nuestros datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Se requiere de forma imprescindible que tengamos una cuenta de acceso seguro en la máquina con la que nos queremos comunicar.

VPN interna

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red interna de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas.

Un ejemplo muy clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal habilitado pueda acceder a la información.

Protocolos para usar VPNs

El protocolo estándar es el IPSEC, pero también tenemos PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados. Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

IPSec

IPSec brinda la seguridad que el protocolo IP no tiene. IPSec da protección a los datos transferidos y garantiza que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

Tiene dos modos de encripción: túnel y transporte. El modo túnel encripta el encabezado y el contenido de cada paquete mientras que el modo de transporte solo encripta el contenido. IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- *Identificación de usuario.*- La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.
- *Administración de direcciones.*- La VPN debe establecer una dirección del cliente en la red privada y cerciorarse que las direcciones privadas se conserven así.
- *Codificación de datos.*- Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.
- *Administración de claves.*- La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.
- *Soporte a protocolos múltiples.*- La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet(IP), el intercambio de paquete de internet(IPX) entre otros.

Ventajas de una VPN

Dentro de las ventajas más significativas podremos mencionar:

- Integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente VPN.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

2.2.2.9 Redes de área local virtuales (VLAN, Virtual Local Area Network)

Cada día es más habitual en todo tipo de organizaciones, dividir su red en diferentes subredes. En esta situación es recomendable incrementar los niveles de seguridad de las zonas más comprometidas, por ejemplo, un servidor donde se almacenen expedientes o datos administrativos del personal.

La característica principal de una LAN es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda. Cuando utilizamos un hub dentro de una red, ésta se puede ver como una red de distribución, donde las estaciones de trabajo utilizan cierto ancho de banda, y mientras más máquinas existan en esa LAN, menor será la cantidad que podrán utilizar. Puede ocurrir que en algún momento el medio esté ocupado por la transmisión de información por parte de alguna de las computadoras, y si otra quiere enviar información en ese preciso momento, no lo podrá hacer hasta que el medio se encuentre disponible. Por otro lado, si dos computadoras determinan que el medio está vacío enviarán su información, pero debido a que éste es compartido puede suceder que los datos se encuentren, habrá una colisión y el material se destruirá; al perderse tendrá que volverse a enviar, lo que llevará a muchas retransmisiones de información. Al segmento conectado por ese hub se le llama dominio de colisiones.

Con objeto de evitar las colisiones, el empleo de un switch mejora el rendimiento de la red debido a que este dispositivo segmenta o divide los dominios de colisiones; cada computadora tiene un enlace individual con el punto central de distribución que es el switch, cada uno de los puertos está destinado a cada una de las computadoras dentro de la red, donde cada una dispone de toda la anchura de banda que la red proporciona.

Algo que no puede evitar ni el switch, ni el hub, es el envío de mensajes de broadcast. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta; estos mensajes los "escuchan" todas las computadoras del segmento, sin excepción, pues son enviados a través de todos los puertos de un hub o de un switch; pero sólo podrá contestarlo la que se está buscando. Ver Figura 2.7

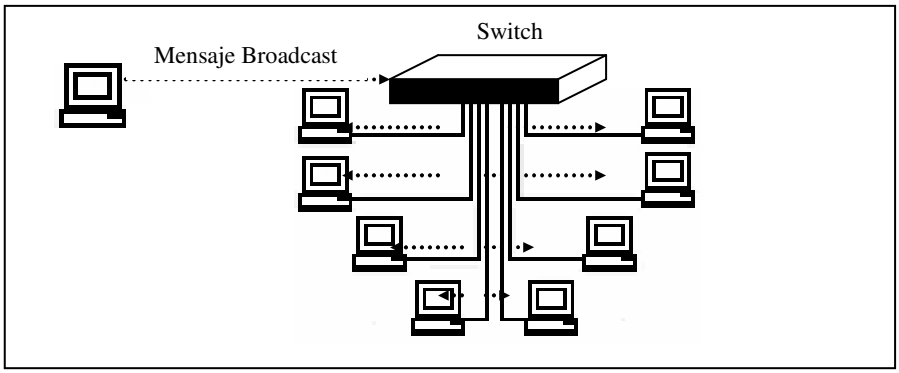


Figura 2.7 Dominio de broadcast

Estos mensajes de broadcast son tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro de la LAN.

Para solventar dicha situación se crea el concepto de VLANs, configuradas dentro de los switches, que dividen en diferentes dominios de broadcast a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.

Una VLAN puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma LAN.

Con el switch, el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los "dominios de colisión" por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los "dominios de broadcast", en lugar de uno solo, se puede configurar el switch para que existan más "dominios".
- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.
- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.
- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán "vernos" como una Red de Área Local independiente a las demás.
- Hasta aquí ya hemos hablado de que se aísla el tráfico de colisiones y de broadcast, y que cada VLAN es independiente una de otra, sin embargo muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLANs. Por ejemplo, los de sistemas con los de redes, o los de nómina con finanzas, etcétera. Para llevar a cabo esta comunicación se requerirá de un router dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente.

Capítulo 3

Estrategias de implementación y administración de la seguridad informática

3.1 Estrategias de implementación de seguridad de la información.

La implementación de un buen sistema de seguridad requiere el uso de las mejores prácticas de la industria. Debe ser escalable, adaptándose a las particularidades y complejidad de las organizaciones y debe ser independiente de la tecnología.

La seguridad en las PyMEs puede ser desde una simple clave de acceso (contraseña) hasta sistemas más complejos, siempre manteniendo la relación de costo-beneficio en los sistemas de información. En las PyMEs, las redes y sistemas suelen ser una LAN aislada, algunas cuentan con un firewall para definir accesos y con ello creen que ya están resguardadas. Incluso algunas ofrecen servicios hacia el exterior como correo electrónico y páginas Web, y por lo regular sitúan a los servidores en una zona desmilitarizada entre el router exterior y la red interna.

Si se trata de PyMEs con varias sucursales que deben estar conectadas de modo seguro es indispensable recurrir a VPNs, canales de comunicación seguros dentro de una red insegura como lo es Internet. Así mismo, en el caso de las PyMEs que cuentan con usuarios móviles que deben comunicarse de modo seguro y privado con los servicios de la red corporativa, por ejemplo ejecutivos que conectarán por medio de la red pública (Internet).

La mala elección de sistemas de comunicación para envío de mensajes de alta prioridad de la empresa pudiera provocar que no alcancen el destino esperado o bien se intercepte el mensaje en su tránsito.

3.1.1 Fase 3: Implementación

Podemos afirmar que la consecuencia directa tanto de nuestro análisis de riesgos como de nuestra política de seguridad, es realizar una implantación, la cual se refiere a una serie de acciones para proveer el marco de seguridad, dichas acciones deben llevar un orden adecuado que permita una utilidad real para nuestra organización.
Al conocer el resultado de nuestro análisis de riesgos, no basta conocer los puntos débiles o vulnerables, tampoco basta con realizar una política de seguridad muy completa. Sino que se debe instalar herramientas, divulgar reglas, concienciar a los usuarios sobre el valor de la información, configurar los controles de acceso, realizar acciones sobre seguridad física de los equipos, etc. Debemos elegir e implementar cada medida de protección, para contribuir con la reducción de las vulnerabilidades. Cada medida debe seleccionarse de tal forma que, al estar en funcionamiento, logre los propósitos definidos. Estos propósitos tienen que ser muy claros.

Lo primero a implementar es la política de seguridad, para ello de debe tener una buena estrategia de divulgación entre los usuarios: Campañas de concienciación, entrenamientos, charlas de divulgación y sistemas de aprendizaje para hacer de la seguridad un elemento común a todos. Un ejemplo común es solicitar a los usuarios el cambio de su contraseña constantemente y que ésta deba tener una complejidad adecuada para la información manejada.

La implementación de la política de seguridad debe ser constantemente monitoreada. Será necesario hacer ajustes de los problemas encontrados, reclamaciones de empleados o informes de auditorías. Se debe también adaptar la seguridad a las nuevas tecnologías, a los cambios administrativos y al surgimiento de nuevas amenazas.

Una política se encuentra bien implantada cuando:

- Refleja los objetivos de la organización, es decir, está de acuerdo con la operación necesaria para alcanzar las metas establecidas.
- Agrega seguridad a los procesos de la organización, permite un buen entendimiento de las exigencias de seguridad y garantiza una gestión inteligente de los riesgos.
- Está sustentada por el compromiso y el apoyo del área administrativa de la organización.

Ahora bien, después de haber establecido nuestra política debemos de seguir dos planes para poder implementarla correctamente en nuestra organización. Los planes a los que nos referimos, son el plan de seguridad y el plan de acciones.

3.1.1.1 Plan de Seguridad

A partir de la política de seguridad, se definen qué acciones deben implementarse (herramientas de software o hardware, campañas de toma de conciencia, capacitación, etc.), para alcanzar un mayor nivel de seguridad.

Estas acciones deben estar incluidas en un plan de seguridad para dar prioridad a las acciones principales en términos de su impacto en los riesgos en que se quiere actuar, con el tiempo y costo de implementación, para establecer así las acciones de corto, mediano y largo plazo.

El plan de seguridad se debe apoyar en un cronograma detallado y contener para cada acción los puntos que enseguida se describen brevemente en la tabla 3.1.

PUNTOS A CONSIDERAR	DESCRIPCIÓN
El riesgo que se desea atenuar	Si la información es susceptible a ciertos ataques, enfocar las acciones a la disminución de estas amenazas.
Los objetivos de seguridad	Se basan en las mejores prácticas del mercado, en estándares y normas de seguridad y en la política de seguridad definida
El(los) activo(s) involucrado(s)	Se puede implementar una herramienta de software (por ej. un firewall) para proteger un servidor de base de datos que contenga información crítica al negocio. En este caso, el activo a ser protegido es la base de datos.
Aumentar la toma de conciencia de los empleados	Implementar un tipo de entrenamiento con relación a la seguridad en donde el activo involucrado son los empleados de la empresa.
Análisis costo-beneficio	Tener justificada, en función de los objetivos de seguridad, la relación costo-beneficio; tomar en consideración: ▪ Tiempo de implementación ▪ Los recursos necesarios (humanos y materiales)
Aspectos críticos previstos para la implementación y cómo superarlos	Prepararse para enfrentar situaciones adversas. (Por ej. la implementación de un firewall, puede requerir sacar un servidor importante por algunos instantes)
Riesgo residual	Considerar lo que puede suceder después de la implementación y estar preparados.
Indicadores para el seguimiento (monitoreo)	Señalar qué indicadores se usan para medir la efectividad y continuidad de la medida implementada y controlar el riesgo. La instalación de un sistema que permita monitorear todo el desempeño de su red.
Responsable(s)	Señalar el responsable de la operación y control de la implementación y de mantener el nivel de seguridad de las medidas implementadas.

Tabla 3.1. Puntos a considerar en un plan de seguridad

3.1.1.2 Plan de acción

Una vez definido y aprobado el plan de seguridad, se parte hacia la definición del plan de acción de las medidas que se deben implementar.

Un plan de acción puede tener varios formatos, pero debe poseer las siguientes características:

- *Objetivos bien definidos*.- De tal forma que sean alcanzados.
- *Escrito de forma correcta*.- Claro y conciso, sin permitir dudas, ni dobles interpretaciones.
- *Coherencia*.- Las actividades están relacionadas y debe existir armonía entre las situaciones, eventos e ideas, de tal manera que nada se disperse del foco. De la unidad y correlación de las proposiciones depende el alcance de los objetos.
- *Secuencia*.- Debe contar con un camino previamente definido que permita la integración de las actividades al racionalizar los esfuerzos y optimizar el tiempo.
- *Flexibilidad*.- Debe prever contingencias durante la ejecución de las tareas y del proceso como un todo. Es necesario estructurarlo de tal manera que permita insertar o actualizar puntos y/o actividades que enriquezcan o faciliten la implementación como las nuevas tecnologías que surjan. Con frecuencia es necesario suprimir algo, pero eso no significa el fin del plan. Los ajustes se realizan sin que el plan pierda su eje.

Metodología de Implementación

Al realizar la implementación propiamente dicha, es muy importante seguir una metodología, que:

1) Defina cómo dar los pasos necesarios para ejecutar un plan de acción

Algunas de las cosas a implantar (aplicaciones, equipos, campañas de divulgación y toma de conciencia entre otras) pueden durar varios días y afectar a varios ambientes, procesos y personas de la organización.
En esos casos, siempre es útil una planificación por separado.

2) Mantenga un mismo estándar de calidad en la implementación sin importar quién lo esté ejecutando.

Es importante definir cómo se realiza el seguimiento del progreso de la implementación y, en caso de dificultades, saber qué acciones tomar y quién debe ser notificado.

Plataforma de Pruebas

En algunos casos, una plataforma de pruebas es necesaria para evaluar la solución y reducir los posibles riesgos sobre el ambiente de producción.
En el caso de las pruebas, podemos mencionar la implantación de un laboratorio para revisar diferentes soluciones antivirus, que nos permita valorar su eficacia y facilidad de administración.

Después de conocer estos planes, ahora nos enfocaremos en las acciones en concreto para poder aminorar las vulnerabilidades en nuestra organización. En estas acciones encontramos el proceso de "hardening" a nuestros equipos de cómputo, el uso de herramientas para el control de accesos (firewalls), el uso de VPN's para comunicarnos forma segura, entre otros.

3.1.1.3 Hardening

Al proceso de reforzamiento de la seguridad en el ámbito tecnológico se le conoce como hardening; se revisa toda la configuración de un equipo para aumentar el nivel de seguridad y hacer más difícil a un atacante poder acceder al sistema.

Los primeros pasos de hardening se deben realizar desde la instalación del sistema operativo: Eliminación de servicios vulnerables o innecesarios, parchar los agujeros de seguridad y asegurar los controles de acceso; una vez terminado esto es necesario realizarlo en todos los demás activos. El hardening es un proceso continuo, en el cual deben eliminarse las vulnerabilidades encontradas en el análisis de seguridad y ser constantemente comprobado y actualizado.

Es necesaria la intervención experta en seguridad, para garantizar que dicha configuración es totalmente segura y que de esta manera se prevendrán riesgos asociados directamente con los problemas tecnológicos.

Dentro de los activos tecnológicos por asegurar, podemos listar los siguientes:

Estaciones de trabajo

Normalmente los equipos vienen con una configuración por defecto que en la mayoría de los casos es insegura, deben ser configurados para evitar que permitan la acción de amenazas.

- Protector de pantallas bloqueado por clave. Permite que las máquinas dejadas solas no sean utilizadas por personas no autorizadas;
- Eliminar configuraciones de seguridad que permitan la instalación o ejecución de ficheros maliciosos;
- Periodicidad de actualización de programas antivirus,
- Forma de organización de los directorios, presencia o ausencia de documentos confidenciales,
- Forma de utilización de la estructura de servidores de ficheros, que garanticen de una manera más eficiente su disponibilidad.

Servidores

Son analizados con prioridades en relación a sus normas de acceso definidas. Se revisan cuáles son los tipos de usuarios que tienen derechos a cierto tipo de información, con base en la clasificación y con relación a la confidencialidad de la información para identificar el exceso o falta de privilegios para la realización de tareas. El enfoque principal se encuentra en los ficheros de configuración y de definición de usuarios que tienen derechos de administración, ya que son los privilegios de administración los que más amenazan los entornos de tecnología y también son los más anhelados por los invasores. La interacción que estos servidores tienen con las estaciones de trabajo de los usuarios, con las bases de datos y con las aplicaciones que respalda son el objeto de hardening de servidores,

independientemente de sus funciones: como ficheros, correo electrónico, FTP, Web y otras.

Equipos de conectividad (routers, switches y otros)

Corregir configuraciones que pongan en riesgo las conexiones realizadas por la red de comunicación que respalda un proceso de negocio.

Estos equipos deben poseer un nivel de seguridad muy alto, pues por lo general se sitúan en la entrada de una red de comunicación. Al aplicarse un alto nivel de configuración a estos activos, el acceso externo a la red del proceso de negocio, estará naturalmente más protegido.

Conexiones

La comunicación entre las redes debe ser segura. Para eso, es importante asegurar la forma con que las conexiones están configuradas y dispuestas en la representación topológica de la red. Esto garantiza que la comunicación sea realizada en un medio seguro, encriptado si fuere necesario, libre de posibilidades de rastreo de paquetes o mensajes, y también como el desvío de tránsito para otros destinos indeseados.

Bases de datos

Representan un elemento de importancia extrema en la cadena comunicativa, pues almacenan informaciones relativas a los procesos de negocio.

Deben ser reforzados los niveles de CIA de la información que allí está, cubrir las necesidades de protección y configuración de seguridad.

Asegurar los privilegios de los usuarios con relación a los permisos de uso, principalmente en lo que se refiere al acceso de aplicaciones que hacen la lectura y escritura de estas informaciones.

Aplicaciones

Son la interfaz entre usuarios e información. Debe garantizar un acceso restrictivo con base en los privilegios de cada usuario y la información que manipulan; garantizar que sus configuraciones estén de acuerdo con los principios de seguridad.

Asegurar la manera en que lee, guarda y transmite la información.

Analizar la forma cómo fue desarrollada o actualizada dicha aplicación.

Por supuesto, dentro del hardening debemos contemplar el aseguramiento de la configuración de los elementos de protección perimetral como los firewalls y los detectores de intrusos.

3.1.1.4 Herramientas para el control de accesos

Vamos a definir las pautas para implementar un sistema de seguridad distribuido, capaz de generar respuestas automáticas, alarmas, o simplemente logs a distintos niveles de nuestra arquitectura de red.

El primer punto donde implantaremos un sensor para detectar ataques y actuar a tiempo es el router de frontera. Ver figura 3.1.

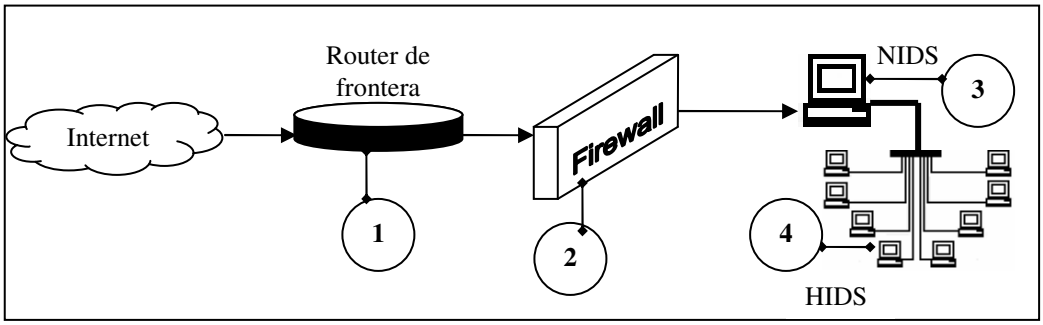


Figura 3.1: Barreras de protección

1) Router de frontera

Lo primero en la implementación de una arquitectura de seguridad general es el router de frontera; es un dispositivo prácticamente imprescindible en las organizaciones modernas, ya que es el que permite conectar una red corporativa a Internet y realiza un filtrado básico de paquetes que se encarga de disminuir la carga del firewall; de este modo se optimizan las características de ambos dispositivos. Este router actúa como gateway de la red interna, recogiendo todos aquellos paquetes de datos destinados a máquinas externas.

Como hemos dicho antes una aplicación adicional de los routers es actuar como firewall, un choke point filtrando paquetes, denegando o permitiendo el flujo de tramas entre la red interna y la red exterior, de acuerdo a unas reglas predefinidas. Con ello se pretenden proteger las redes corporativas frente a entradas o salidas no autorizadas. Configurando correctamente este router podremos evitar posibles ataques.

Las reglas son extremadamente sencillas y se implantan de forma muy eficiente en cualquier router de frontera:

- *Reglas a aplicar a los paquetes que entran en nuestra red.-* Deben filtrarse todos los paquetes entrantes cuya dirección de origen sea inválida por pertenecer a los rangos asignados a redes privadas y aquellas cuyo destino sea la dirección broadcast de nuestra red.
- *Reglas a aplicar a los paquetes que salen de nuestra red.-* No debe permitirse que ningún paquete malicioso abandone nuestra red, de forma que pueda atacar otras. No debemos dejar salir ningún paquete cuya dirección IP fuente no pertenezca a nuestra red.

2) Firewall

La segunda barrera de protección, ver figura 3.1, será el firewall y es aquí donde vamos a implantar el primer sistema de respuesta automática ante ataques, esta

respuesta será habitualmente el bloqueo de la dirección atacante en el propio firewall.

La configuración y el nivel de seguridad serán distintos en una empresa que utilice un firewall para bloquear todo el tráfico externo hacia el dominio de su propiedad frente a otra donde sólo se intente evitar que los usuarios internos pierdan el tiempo en la red, bloqueando por ejemplo todos los servicios de salida al exterior excepto el correo electrónico. Pero en cualquier caso la configuración del o los firewalls de la organización se lleva a cabo con base en el manual de políticas de seguridad definidas para la empresa, y sobre esta decisión influyen, además de motivos de seguridad, motivos administrativos de cada organismo.

En función del valor estimado de lo que deseemos proteger, debemos gastar mayor o menor cantidad de dinero, o no gastar nada. Un firewall puede no representar gastos extras para la organización, o suponer un gran desembolso; se puede utilizar una PC o un router como firewall, sin gastarse nada en él excepto unas horas de trabajo, pero esto evidentemente no funciona cuando el sistema a proteger es una red de tamaño considerable. No es recomendable a la hora de evaluar el dinero a invertir, fijarse sólo en el costo de su instalación, sino también en el de su mantenimiento. Existen dos métodos para implementar un firewall:

Firewall de red basado en host

Los proveedores utilizan dos maneras de implementar software de firewall en plataformas de hardware de servidores. Una de ellas es una aplicación de software basado en una plataforma existente y conocida, así por medio de una aplicación más obtenemos los beneficios de un firewall. Antes de implementarlo es necesario asegurar el sistema operativo sobre el que se instalará. La mayoría de estas aplicaciones realizan pasos adicionales como la sustitución o modificación de la pila TCP/IP, modificar los archivos de inicio, entradas de registro y agregar nuevos procesos.

La segunda opción es un sistema operativo con firewall integrado. No tiene todas las funciones de un sistema operativo normal ya que se elimina todo aquello que no sea necesario para el funcionamiento del firewall. Es más seguro que la primera opción pero obliga a comprender un nuevo sistema operativo

Dispositivos Firewall (appliance)

Contiene hardware y software optimizado específicamente para su función. Pueden utilizar un disco duro para almacenar el sistema operativo y la aplicación firewall, o bien, los almacena en un chip o tarjeta flash, de forma muy parecida al BIOS de una PC. Se configuran mediante la interfaz de línea de comandos, una herramienta propietaria o una interfaz basada en Web que se ejecuta en HTTPS.

Las políticas de accesos en un firewall se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad y protegernos de cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenirse.

La regla básica de un firewall es asegurar que todas las comunicaciones entre la red propia e Internet se realicen conforme a las políticas de seguridad de la organización, para lo que evalúan cada paquete que atraviesa la frontera entre el interior y el exterior de la red.

Estas reglas de filtrado de paquetes se expresan como una tabla de condiciones y acciones que se consulta en orden hasta encontrar una regla que permita tomar una decisión sobre el bloqueo o reenvío de la trama; ciertas implementaciones permiten indicar si el bloqueo de un paquete se notificará a la máquina origen mediante un mensaje ICMP.

Los siguientes procedimientos nos ayudan a prevenir errores al generar las reglas y facilita la administración, ya que la especificación incorrecta de estas reglas constituye uno de los problemas de seguridad habituales.

A) Agrupar servicios y equipos

Si el dispositivo permite agrupar servicios (puertos de origen y destino) y direcciones IP, es recomendable hacerlo. Los grupos deben estar relacionados preferentemente con unidades y servicios organizacionales que sean fáciles de identificar. Agrupar no sólo reduce el número de reglas en sí, también evita errores en la administración ya que cambios posteriores requieren únicamente agregar o eliminar elementos en los grupos, en vez de cambiar los filtros.

B) Definir reglas

Las reglas serán únicamente filtros que permiten explícitamente actividades legítimas del negocio, por ejemplo: permitir tráfico de Internet al puerto 80 de los servidores Web. Veamos una hipotética tabla de reglas de filtrado. Tabla 3.2

Origen	Destino	Tipo	Puerto	Acción
158.43.0.0	*	*	*	Deny
*	195.53.22.0	*	*	Deny
158.42.0.0	*	*	*	Allow
*	193.22.34.0	*	*	Deny

Tabla 3.2 Tabla de reglas de filtrado de paquetes

Revisando el ejemplo dado en la tabla 3.2, si llega un paquete proveniente de una máquina de la red 158.43.0.0 se bloquearía su paso, sin importar el destino de la trama; de la misma forma, todo el tráfico hacia la red 195.53.22.0 también

se detendría. Pero, ¿qué sucedería si llega un paquete de un sistema de la red 158.42.0.0 hacia 193.22.34.0? Una de las reglas nos indica que dejemos pasar todo el tráfico proveniente de 158.42.0.0, pero la siguiente nos dice que si el destino es 193.22.34.0 lo bloqueemos sin importar el origen. En este caso depende de nuestra implementación y del orden de análisis que siga: si se comprueban las reglas desde el inicio, el paquete pasaría, ya que al analizar la tercera entrada se finalizarían las comprobaciones; si operamos de modo contrario, de abajo hacia arriba, el paquete se bloquearía puesto que encontramos el bloque antes. Como podemos ver, ni siquiera en una tabla tan simple las cosas son obvias, por lo que si extendemos el ejemplo a un firewall real podemos hacernos una idea de hasta que punto hemos de ser cuidadosos con el orden de las entradas de nuestra tabla.

C) Definir excepciones a las reglas

Las excepciones son negaciones particulares o generales (*reject o drop*) para las reglas, por ejemplo: rechazar tráfico desde Internet hacia cualquier puerto de cualquier servidor interno, si la IP de origen está en el rango de IPs reservadas.

D) Ordenar y optimizar la configuración

Las reglas se aplican en orden secuencial, por esta razón el orden es de suma importancia; se deben ordenar los elementos de acuerdo a la frecuencia con la que son aplicados, de manera que aquellos que se aplican con mayor frecuencia estén al principio.

a. Implementar las excepciones a las reglas, debe ser lo primero que se revise en la secuencia de filtros.
b. Implementar las reglas.
c. Implementar la política por omisión. En la secuencia de filtros, la política por omisión debe aplicarse siempre y sin excepciones al final.

Siempre hemos de tener presente el orden de análisis de las tablas para poder implementar la política de seguridad de una forma correcta; cuanto más complejas sean las reglas, más difícil será para el administrador implementarlas. Independientemente del formato, la forma de generar las tablas dependerá obviamente del sistema sobre el que se esté trabajando, por lo que es indispensable consultar su documentación.

E) Establecer política por omisión

Si al final de la secuencia de reglas no se aplicó ninguna, debe haber una acción por omisión, y ésta es definida por la política por omisión; es decir, define el comportamiento cuando no hay más reglas por procesar.

Para evitar problemas lo mejor es insertar siempre una regla por defecto al final de nuestra lista, o al inicio según la cuestión del orden, con la acción que

deseemos realizar por defecto; si por ejemplo deseamos bloquear el resto del tráfico que llega, y suponiendo que las entradas se analizan en el orden habitual, podríamos añadir a nuestra tabla la siguiente regla. Ver Tabla 3.3

Origen	Destino	Tipo	Puerto	Acción
*	*	*	*	Deny
*	195.53.22.0	*	*	Deny
158.42.0.0	*	*	*	Allow
*	193.22.34.0	*	*	Deny
*	*	*	*	Deny

Tabla 3.3 Regla de implementación de política por omisión

Las mejores prácticas recomiendan que esta política se configure de manera que se niegue el acceso a cualquier tipo de tráfico. Con esta configuración se espera que el administrador defina reglas para permitir el paso de tráfico legítimo, y la política por omisión se encargará de negar el resto del tráfico (ilegítimo); pero esto no siempre sucede así, diferentes implementaciones ejecutan diferentes acciones, algunas deniegan el paso por defecto, otras aplican el contrario de la última regla especificada; es decir, si la última entrada era un Allow se niega el paso de la trama, y si era un Deny se permite, otras dejan pasar este tipo de tramas. Muchos dispositivos incluyen la política de forma implícita.

Conociendo las direcciones origen y destino y el puerto destino de una conexión ya podemos detectar cierto tipo de ataques; por ejemplo los escaneos de puertos, tanto horizontales como verticales, que se lanzan contra nuestros sistemas. La técnica de detección de estos ataques está basada en comprobar determinados eventos de interés dentro de una ventana de tiempo; así, cuándo una misma dirección origen accede a un determinado puerto de varios destinos en menos de un cierto tiempo (escaneo horizontal) o cuando esa misma maquina accede a diferentes puertos bien conocidos de un mismo sistema también en menos de ese tiempo (escaneo vertical).

Una técnica alternativa que suele ser utilizada con bastante efectividad para detectar escaneos verticales consiste en vigilar el acceso a determinados puertos de los sistemas protegidos por el firewall, acceso que con toda probabilidad representará un intento de violación de nuestras políticas de seguridad. Otro tipo de ataques que también son fácilmente detectables vigilando el acceso a determinados puertos de nuestros sistemas protegidos son aquellos que detectan la presencia de diferentes troyanos.

En la tabla 3.4 se muestran algunos de los puertos a los que conviene estar atentos a la hora de implementar una política de detección de intrusos en nuestro firewall; por supuesto, existen muchos más que pueden ser considerados sospechosos, pero en cualquier caso siempre conviene ser muy precavido con su monitoreo ya que algunos de ellos pueden ser usados por

usuarios lícitos a los que causaríamos una grave negación de servicio si, por ejemplo, les bloqueáramos el acceso a nuestra red a causa de un falso positivo.

Servicio	Puerto	Protocolo	Ataque
Ttymux	1	TCP	Escaneo horizontal
Echo	7	TCP/UDP	Escaneo horizontal
Systat	7	TCP	Escaneo horizontal
Daytime	13	TCP/UDP	Escaneo horizontal
Netstat	15	TCP	Escaneo horizontal
Finger	79	TCP	Escaneo horizontal/vertical
Who	513	UDP	Escaneo horizontal
Uucp	540	TCP	Escaneo horizontal/vertical
NetBus	12345	TCP	Troyano
NetBus	12346	TCP	Troyano
NetBus	20034	TCP	Troyano
BackOrifice	31337	UDP	Troyano
Hack´a´Tack	31789	UDP	Troyano
Hack´a´Tack	31790	UDP	Troyano

Tabla 3.4: Algunos puertos a monitorizar en un firewall

Esta barrera de detección de intrusos es realmente útil, pero también insuficiente frente a determinados ataques; entonces entra en juego el tercer nivel del sistema de detección de intrusos, el ubicado en el segmento de red.

3) IDS de red (NIDS, Network Intrusion Detection Systems)

Una cuestión típica es si debemos colocarlo detrás o delante del firewall que protege a nuestra red. Si dejamos que el sensor analice el tráfico antes de que sea filtrado en el firewall, podremos detectar todos los ataques reales que se lanzan contra nuestra red, sin ningún tipo de filtrado que pueda detener las actividades de un pirata; no obstante, no nos interesa detectar todos estos intentos de ataque, sino detectar el tráfico sospechoso que atraviesa nuestro firewall y que puede comprometer a nuestros servidores. Por tanto, es recomendable colocar el sensor de nuestro sistema de detección de intrusos en la zona protegida. Ver figura 3.1

Como el sensor ha de analizar todo el tráfico dirigido a las máquinas protegidas, si nos encontramos en un entorno donde dichas máquinas se conecten mediante un hub o mediante otras arquitecturas en las que cualquiera de ellas vea, o pueda ver, el tráfico de las demás, no hay muchos problemas de decisión sobre dónde situar al sensor: lo haremos en cualquier parte del segmento. Sin embargo, si nuestros sistemas se conectan con un switch la cuestión se complica un poco, ya que en los puertos de este elemento se verá únicamente el tráfico dirigido a las máquinas que estén conectadas a cada uno de estos; en este caso, es necesaria la replicación de puertos que se puede configurar en la mayoría de los switches; es decir, todo el tráfico dirigido a determinado puerto se duplicará en otro donde colocaremos el sensor para monitorear el tráfico.

La interfase de red por donde se analiza el tráfico no tiene por qué tener dirección IP. Perfectamente podemos tener una interfase de red levantada e inicializada pero sin asignarle ninguna dirección. Esto nos puede resultar útil si no nos interesa que en el segmento protegido se detecte una nueva máquina, o simplemente si no queremos que nuestro sensor sea alcanzable de alguna forma por el resto de sistemas de su dominio de colisión. Para nuestra comodidad, por ejemplo, a la hora de centralizar logs de diferentes sensores, podemos usar una máquina con dos interfaces, una escuchando todo el tráfico y la otra configurada de forma normal, que será por la que accedamos al sistema.

Los NIDS funcionan como sniffers capaces de actuar como sistema de detección de intrusos en redes de tráfico moderado; SNORT es la opción ideal para las PyMEs por su facilidad de configuración, su adaptabilidad, sus requerimientos mínimos y sobre todo que es un software libre, frente a otros sistemas que, aunque quizás sean más potentes, son también mucho más pesados y caros. SNORT monitorea todo un dominio de colisión y funciona mediante detección de usos indebidos. Estos usos indebidos, o al menos sospechosos, se reflejan en una base de datos formada por patrones de ataques; dicha base de datos se puede descargar de la web, será la base para el correcto funcionamiento de nuestro sistema de detección de intrusos.

Una vez instalado y compilado llega el momento de ponerlo en funcionamiento; y es aquí donde se produce uno de los errores más graves en la detección de intrusos. Por lógica, uno tiende a pensar que el sensor proporcionará mejores resultados cuantos más patrones de ataques contenga en su base de datos; nada más lejos de la realidad.

En primer lugar, hemos de evaluar con mucho cuidado si realmente vale la pena sobrecargar la base de datos con patrones que permitan detectar estos ataques, es muy probable que no todos los ataques que el IDS es capaz de detectar sean susceptibles de producirse en el segmento de red monitoreado. Debemos tener presente que el sniffer no detendrá el tráfico que no sea capaz de analizar para hacerlo más tarde, sino que simplemente lo dejará pasar. Si el sensor ha de analizar todo el tráfico, quizás mientras trata de decidir si un paquete entre dos máquinas protegidas se adapta a un patrón estamos dejando pasar tramas provenientes del exterior que realmente representan ataques. Así, debemos introducir en la base de patrones de ataques los justos para detectar actividades sospechosas contra nuestra red.

En segundo lugar, pero no menos importante, es necesario estudiar los patrones de tráfico que circulan por el segmento donde el sensor escucha para detectar falsos positivos y, reconfigurar la base de datos, o bien eliminar los patrones que generan esas falsas alarmas. Si un patrón genera un número considerable de falsos positivos, debemos plantearnos su eliminación: simplemente no podremos decidir si se trata de verdaderas o de falsas alarmas.

Esto es especialmente crítico si lanzamos respuestas automáticas contra las direcciones "atacantes", por ejemplo, detener todo su tráfico en nuestro firewall: aunque en un entorno de alta seguridad quizás vale la pena detener muchas acciones no dañinas con tal de bloquear también algunos ataques, constituiría una negación de servicio contra los usuarios que hacen uso legítimo de nuestros sistemas; en un entorno normal de producción esto es impensable. Seguramente será más provechoso detectar y detener estos ataques por otros mecanismos ajenos al sensor. En resumen, hemos de adaptar a nuestro entorno de trabajo la base de datos de patrones de posibles ataques. Quizá valga la pena destinar el tiempo que sea necesario en esta parte de la implantación, ya que eso nos ahorrará después muchos análisis de falsas alarmas.

4) IDS basados en máquina (HIDS, Host Intrusion Detection Systems)

Si bien un NIDS es vital para proteger cualquier sistema pues con frecuencia suele ser el punto más importante, el que más ataques detecta y el sistema de detección más instalado en entornos reales. No obstante esta enorme importancia suele generar una falsa sensación de seguridad; en muchos entornos los responsables de seguridad, a la hora de trabajar con IDS, se limitan a instalar diversos sensores en cada segmento a proteger, creyendo que así son capaces de detectar la mayoría de ataques. Pero ciertos ataques pueden eludir a estos sensores. Es necesario un nivel adicional en nuestro esquema de detección: justamente el compuesto por los sistemas basados en la propia máquina a proteger. Ver figura 3.1. Tendremos que recurrir a los analizadores de logs, usar un shellscript que procese registros del sistema o de algunas aplicaciones en específico en busca de patrones que puedan denotar un ataque.

El análisis de registros generados por el sistema o por ciertas aplicaciones suele ser una excelente fuente de información de cara a la detección de actividades sospechosas en nuestros entornos, pero no es habitual aplicar dicho análisis en un esquema de respuesta automática ante ataques. Es mucho más común automatizar la revisión de logs para que periódicamente se analicen esos registros y se envíe un mensaje de alerta por correo electrónico a los responsables de seguridad en caso de que algo anormal se detecte; evidentemente no es un modelo que trabaje en tiempo real, pero no por ello deja de ser un esquema útil en la detección de intrusos; el único problema que se presenta a la hora de realizar el análisis suele ser la decisión de qué patrones buscar en los registros, algo que depende por completo del tipo de log que estemos analizando.

Nuevos sistemas han sido desarrollados para resolver las ambigüedades y huecos al sólo tener un monitoreo pasivo del tráfico de la red. Los IPS (Intrusión Prevention Systems) son considerados como una extensión de los IDS, los cuales analizan todo el tráfico, pero añaden la funcionalidad de bloquear en línea todo el tráfico que consideren pone en riesgo la seguridad. Para mayor información de los IPS puede ver en apéndice.

3.1.1.5 Implementación de VPN

En caso de ser necesaria la implementación de una VPN todas las opciones disponibles en la actualidad caen en tres categorías básicas:

- Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Nortel, Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, D-link etc.
- En el caso basado en firewalls, se obtiene un nivel de seguridad alto por la protección que brinda el firewall, pero se pierde en rendimiento. Muchas veces se ofrece hardware adicional para procesar la carga VPN. Por ejemplo: Checkpoint NGX, Cisco Pix, Juniper.
- Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas la operación de los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, Linux y los Unix en general. Por ejemplo productos de código abierto (Open Source) como OpenSSH, OpenVPN y FreeS/Wan.

3.1.1.6 Otras acciones que pueden implementarse

De acuerdo a los requerimientos de cada organización pueden implementarse otras acciones de defensa. Ver tabla 3.5.

ACCIÓN	DESCRIPCIÓN
Control de acceso a los recursos de la red	Implementación de controles en las estaciones de trabajo que permiten la gestión de acceso, en diferentes niveles, a los recursos y servicios.
Seguridad para equipos portátiles	Implantación de aplicaciones y dispositivos para la prevención contra accesos indebidos y el robo de información.
ICP – Infraestructura de llaves públicas	Emplear servicios, protocolos y aplicaciones para la gestión de llaves públicas, que suministren servicios de criptografía y firma digital
Seguridad en correo electrónico	Certificados digitales para garantizar la CIA, software para filtrado de contenido; proteger de aplicaciones maliciosas que llegan vía correo.
Seguridad para las aplicaciones	Implementación de dispositivos y aplicaciones para garantizar la CIA, además del análisis de las vulnerabilidades de la aplicación, al suministrar una serie de recomendaciones y estándares de seguridad.
Seguridad en comunicación Móvil	Acceso a Internet para usuarios de aparatos móviles como teléfonos celulares y PDA's, para permitir transacciones e intercambiar información con seguridad vía Internet.
Seguridad para servidores	Configuración de seguridad en los servidores, garantizar un control mayor en lo que se refiere al uso de servicios y recursos disponibles.
Firewall interno	Este firewall funciona al aislar el acceso a la red de servidores críticos, minimizando los riesgos de invasiones internas a servidores y aplicaciones de misión crítica.

Tabla 3.5: Resumen de algunas otras acciones que pueden implementarse

3.2 Estrategias de administración de seguridad de la información.

La seguridad de la información, para que sea efectiva, debe estar soportada por un conjunto de procesos formales diseñados expresamente para cumplir con los objetivos de seguridad que hayan sido definidos por la organización y aun cuando la tecnología es parte fundamental para resolver los problemas de seguridad, la seguridad no es un problema de tecnología, es un problema de administración.

El hecho de que la organización tenga implementados firewalls, soluciones de antivirus y sistemas de detección de intrusos en las zonas de mayor sensibilidad no significa que se solucionen completamente los problemas de seguridad

Los Objetivos de la administración de la seguridad son:

- Proporcionar servicios de seguridad a los elementos de la red.
- Crear estrategias para la prevención y detección de ataques.
- Crear estrategias para la respuesta a incidentes.

3.2.1 Fase 4: Administración

Los puntos principales a considerar al manejar y controlar recursos y atributos de seguridad con el fin de asegurar la protección de la información son:

Evitar soluciones fragmentadas

Cada solución de seguridad no debe ser diseñada e implementada independientemente del resto de las soluciones instaladas en la organización. Deben integrarse entre sí. Evitar que diferentes grupos implementen diferentes soluciones para un mismo problema dentro de la misma organización.

Tener una visión estratégica

Saber que se va a hacer en el corto, mediano y largo plazo en materia de seguridad para lograr los objetivos planteados

Comprometer a todas las áreas

Es muy común encontrar que las iniciativas de seguridad nacen de las áreas de sistemas. Cuando estas iniciativas tienen que salir e implementarse en otras áreas de la organización, se enfrentan muchos problemas para que se adopten e implementen estas iniciativas.

Contar con medidas de control de desempeño

Mecanismos para medir el desempeño de las soluciones de seguridad que se implementan (monitoreo).

Personal especifico para la seguridad

Evitar que los que administran los firewalls o los IDS sean los mismos que administran los servidores, las bases de datos y las comunicaciones.

Existe un estándar llamado ISO/IEC 27001, sucesor al ISO/IEC 17799, que define todas las propiedades y funciones que debe tener este sistema de administración para la seguridad informática, que en terminología del estándar se conoce como ISMS, por las siglas en inglés de Information Security Management System.

Lo más importante es que el estándar obliga a pensar sobre lo que ésta debe hacer con base en los perfiles de riesgo de cada uno de los activos de la organización y en todo momento también obliga a la organización a documentar las razones de la aplicación de algún control.

Políticas y Procedimientos relacionados con la administración

- Políticas de seguridad (contraseñas y listas de acceso)
- Procedimiento manejo de incidentes.
- Procedimiento de eventos de soporte.
- Procedimiento de control de cambios.
- Planes de contingencia y continuidad (Políticas de respaldo)

3.2.1.1 Monitoreo

Implementación de sistemas y procesos para la gestión de los eventos de seguridad en el ambiente tecnológico, haciendo posible un control mayor del ambiente, para dar prioridad a las acciones e inversiones.

Es indispensable la medición constante de indicadores que muestren qué tan eficaces son las medidas adoptadas y lo que se necesita cambiar. A partir de la lectura de esos indicadores, se hace otro análisis de riesgos y se comienza el ciclo nuevamente como se analizará mas adelante.

Mediante el monitoreo, detección y registro en línea de eventos significativos de la seguridad ocurridos fuera de los parámetros permitidos en nuestras herramientas de seguridad obtendremos información sobre los intentos de ataque que estemos sufriendo (origen, fecha y hora, tipos de acceso), con el fin de facilitar su atención y solución inmediata; así como la existencia de tramas que aunque no supongan un ataque son al menos sospechosas.

Dependerá casi por completo de la política de seguridad a seguir. En función de los datos que nuestros sensores hayan recogido, procesarlos de forma periódica y tomar una determinada acción: bloquear las direcciones atacantes en el firewall, realizar informes o simplemente no hacer nada.

Un correcto monitoreo deberá contemplar al menos los siguientes puntos:

1) **Definición de Alarmas**

¿Qué información debemos registrar? Además de los registros estándar como los que incluyen estadísticas de tipos de paquetes recibidos, frecuencias, o direcciones fuente y destino se recomienda auditar información de la conexión: origen y destino, nombre de usuario, hora y duración; intentos de uso de protocolos denegados, intentos de falsificación de dirección por parte de máquinas internas al perímetro de seguridad, paquetes que llegan desde la red externa con la dirección de un equipo interno y tramas recibidas desde routers desconocidos.

2) **Priorización**

Evaluación de la importancia de una alerta respecto del escenario. Es recomendable asignar un peso específico a cada alarma generada en el sensor, y actuar sólo en el caso de que detectemos un ataque que denote muy claramente un intento de intrusión, o bien varios menos sospechosos, pero cuya cantidad nos indique que no se trata de falsos positivos.

La prioridad de una alerta es dependiente de la topología, políticas de acceso y flujo de datos.

3) **Valoración de activos**

Si existe una conexión sospechosa de un usuario en un servidor:

- Darle máxima prioridad si el usuario es externo e intenta ingresar a información restringida.
- Darle prioridad baja si el usuario es interno y ataca a una impresora.
- Descartarla si es un usuario que normalmente hace pruebas contra un servidor de desarrollo.

4) **Inventario**

Si una alerta que se refiere a un ataque al servicio IIS de Microsoft llega a una máquina con sistema operativo Unix y servidor Apache, la alerta por su puesto no es valida pero debe ser corregida para evitar futuras alertas.

5) **Valoración de amenazas**

No todos los ataques que un sensor detecta tienen la misma probabilidad de serlo realmente: si se detecta un paquete ICMP de formato sospechoso no tiene por qué representar un verdadero ataque.

6) **Valoración de Fiabilidad de cada alerta**

Todos esos registros han de ser leídos con frecuencia, y el administrador de la red ha de tomar medidas si se detectan actividades sospechosas; si la cantidad

de logs generada es considerable nos puede interesar el uso de herramientas que filtren dicha información. Y así determinar la probabilidad de que el ataque detectado sea realmente un falso positivo.

7) Contemplar direcciones `protegidas'

Otro punto a tener en cuenta antes de lanzar una respuesta automática contra un potencial atacante es su origen; si se trata de una dirección externa, seguramente la respuesta será adecuada, pero si se trata de una interna a nuestra red o de empresas colaboradoras, aunque sean externas, la situación no es tan clara. Quizás estaríamos bloqueando el acceso a alguien a quien no deberíamos. Aunque se trate de cuestiones mas políticas que técnicas, es muy probable que en nuestro IDS debamos tener claro un conjunto de direcciones contra las que no se va actuar; si desde ellas se detecta actividad sospechosa, podemos preparar un mecanismo que alerte a los responsables de seguridad y entonces tomar las acciones que consideremos oportunas.

Si nos limitamos a bloquear direcciones, es posible que nosotros mismos causemos una importante negación de servicio a usuarios legítimos. Si nuestro sensor lanza demasiadas respuestas automáticas en un periodo de tiempo pequeño, el propio sistema debe encargarse de avisar a una persona que se ocupe de verificar que todo es normal.

3.2.1.1 Esquema de respuestas automáticas

El propio sensor debe ser capaz de generar respuestas automáticas ante lo que considere un intento de ataque, lo más habitual suele ser un bloqueo total de la dirección atacante en nuestro firewall, unida a una notificación a los responsables de seguridad registrando las medidas tomadas contra una determinada dirección en un log pues es posible que se trate de un usuario autorizado que no atacaba nuestras máquinas, a pesar de que el sensor opine lo contrario. No importa lo seguros que estemos de lo que hacemos ni de las veces que hayamos revisado nuestra base de datos de patrones: nunca podemos garantizar por completo que lo que nuestro IDS detecta como un ataque realmente lo sea.

Debemos diseñar un esquema de respuestas automáticas adecuado. Al detectar un ataque desde determinada dirección, el modelo deberá comprobar que no se ha superado el número de respuestas máximo por unidad de tiempo, si este umbral ha sido sobrepasado no actuaremos de forma automática, para no causar importantes negaciones de servicio, pero si no lo ha superado, se verifica que la dirección IP contra la que se actuará no corresponde a una de nuestras 'protegidas', si es así no actuamos en tiempo real contra la máquina, pero se ha detectado y guardado un log, por lo que un operador puede preocuparse más tarde de investigar la alerta. Si se trata de una dirección no controlada ponderamos la gravedad del ataque: un ataque con poca posibilidad de ser un falso positivo tendrá un peso elevado, mientras que uno que pueda ser una

falsa alarma tendrá un peso bajo; aún así, diferentes ataques de poco peso pueden llegar a sobrepasar nuestro límite si se repiten en un intervalo de tiempo pequeño. Es importante recalcar el que sean diferentes, ya que si la alarma que se genera es todo el rato es la misma debemos plantearnos que posiblemente es un proceso que se ejecuta periódicamente y, por lo tanto, no se trata de un ataque y evidentemente no debemos bloquearlo sin más, seguramente es más recomendable revisar nuestra base de datos de patrones de ataques para ver por qué se puede estar generando continuamente dicha alarma.

Por último, si nuestro umbral no ha sido superado debemos registrar el ataque, su peso y la hora en que se produjo para poder hacer ponderaciones históricas ante más alarmas generadas desde la misma dirección, y si se ha superado el esquema debe efectuar la respuesta automática: bloquear al atacante en el firewall, enviar un correo electrónico al responsable de seguridad, etc. Debemos pensar que para llegar a este último punto, tenemos que estar bastante seguros de que realmente hemos detectado un ataque: no podemos permitirnos el efectuar respuestas automáticas ante cualquier patrón que nos parezca sospechoso sin saber realmente, o con una probabilidad alta, que se trata de algo hostil a nuestros sistemas.

Es muy recomendable que ante cada respuesta se genere un aviso que pueda ser validado por un administrador de sistemas o por responsables de seguridad, mejor si es en tiempo real; por muy seguros que estemos del correcto funcionamiento de nuestro detector de intrusos, nadie nos garantiza que no nos podamos encontrar ante comportamientos inesperados o indebidos, y así darse cuenta de un error y subsanarlo. A través de un proceso continuo de revisión y realimentación, la organización realizará cada vez un mejor filtrado de alertas recibidas por los detectores.

3.2.1.3 Correlacionadores

Cada uno de los modelos de detección y/o respuesta puede actuar de forma independiente sin muchos problemas, pero en los entornos actuales esto es cada vez menos habitual. Hoy día, lo normal es encontrarse arquitecturas de red segmentadas, con sensores en cada segmento tanto a nivel de red como de host, así como uno o varios firewall en los que también se lleva a cabo detección de intrusos y respuesta automática.

El tener elementos independientes no es lo más adecuado, si bien al contar con un sistema de detección de intrusos nos es posible detectar los eventos más concretos, no somos capaces de revisar todas las alertas que estos nos envían debido a dos razones: demasiadas alertas y éstas no son fiables, es decir, obtenemos demasiados falsos positivos.
Definamos una función de correlación como un algoritmo que realiza una operación que recibe diversos datos de entrada y ofrece un solo dato de salida. La información recogida por nuestros detectores y monitores es información

específica pero parcial, mostrando tan solo una parte de toda la información que nos interesaría tener. La capacidad de correlación nos permitirá aprovechar los sistemas al máximo ya que través de una nueva capa de proceso se abarcará toda la información que podría existir de la red.

Para esto necesitamos un esquema capaz de unificar en la misma pantalla y con un mismo formato los eventos de seguridad de un determinado momento, ya sean del Router, el Firewall, del IDS, o del servidor Unix; y ante los ataques detectados, lanzar una sola respuesta automática ante un mismo ataque, aunque se detecte simultáneamente en diferentes sensores. La centralización en una única consola puede ser necesaria para algo tan simple como generar estadísticas mensuales acerca del número de ataques contra nuestro entorno de trabajo. Todos los productos de seguridad poseen la capacidad de gestión centralizada a través de protocolos estándar, la centralización es por lo tanto sencilla utilizando estos protocolos.

También será indispensable un programa de análisis, o traductor, que conozca los tipos y formatos de alertas de los diferentes detectores; será necesario organizar la base de datos para homogenizar el tratamiento y visualización de todos estos eventos; a esto se le conoce como normalización. Así podremos desarrollar procesos que permitan detectar patrones más complejos y distribuidos, relacionar y procesar la información permitiendo aumentar la capacidad de detección, priorizar los eventos según el contexto en que se producen y monitorizar el estado de seguridad de nuestra red.

Los sistemas de correlación cubren la falta de sensibilidad, fiabilidad y la visibilidad limitada de nuestros sensores. Para entender más estos conceptos ver tabla 3.6.

CARACTERÍSTICAS	DESCRIPCIÓN	EFECTO ANTE SU AUSENCIA
Fiabilidad	El grado de certeza que nos ofrece ante el aviso de un posible evento	Falsos positivos
Sensibilidad	La capacidad de análisis en profundidad y complejidad, a la hora de localizar un posible ataque	Falsos negativos

Tabla 3.6: Características de los sensores

Métodos de Correlación

Para lograr estos objetivos utilizaremos dos métodos de correlación:

- *Correlación mediante Secuencias de Eventos*.- Se centra en los ataques conocidos y detectables; relaciona a través de reglas que implementarán una máquina de estados, los patrones y comportamientos conocidos que definen un ataque.
- *Correlación mediante Algoritmos Heurísticos*.- Tomando una aproximación opuesta implementaremos algoritmos que mediante funciones

heurísticas intenten detectar situaciones de riesgo. Este método detectará situaciones sin conocer ni ofrecer detalle de los mismos; será útil para detectar ataques no conocidos y obtener una visión general del estado de seguridad para un amplio número de sistemas.

3.2.1.4 Auditoría

La auditoría de seguridad informática deberá principalmente comprobar la seguridad de los programas en el sentido de garantizar que lo ejecutado por la máquina sea exactamente

a) lo previsto o lo solicitado inicialmente, y
b) cumpla las condiciones que le han sido encomendadas.

Comprende la revisión y la evaluación independiente y objetiva mediante una serie de exámenes periódicos o esporádicos cuya finalidad es analizar y evaluar la planificación, el control, la eficacia y la adecuación de la infraestructura informática de todas o algunas de las áreas de la organización, el cumplimiento de los estándares y procedimientos en vigor, de los objetivos fijados, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos. Se recomienda que para que esta evaluación tenga veracidad sea efectuada internamente y posteriormente comprobaba por externos.

Objetivos

- Evaluar los controles de la función informática
- Analizar la eficiencia de los sistemas
- Verificar el cumplimiento de las políticas y procedimientos
- Revisar que los recursos materiales y humanos se utilicen eficientemente.

Metodología

1. *Plantear alcance y objetivos.*- Deberán definirse de forma clara, detallando no solamente los temas que serán examinados, sino también indicar cuales se omitirán.
2. *Estudio inicial del entorno.*- Detallar los puntos a considerar en la revisión y evaluación de todos los aspectos de seguridad de la información: normas, controles, técnicas y procedimientos. Ver tabla 3.7.
3. *Determinación de los recursos necesarios.*
4. *Elaboración del plan de Auditoría.*- Determina con precisión las actividades a realizar, los responsables de llevarlas a cabo y las fechas de realización.
5. *Actividades propiamente dichas de la auditoría.*- Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito especifico.
6. *Informe Final.*- La emisión de una opinión profesional y obtener recomendaciones para mejorar o lograr un adecuado control interno con el fin de lograr mayor eficiencia operacional y administrativa

Puntos a Considerar	Descripción
Sistemas y Aplicaciones	• Evaluación de los diferentes sistemas en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas). • Evaluación de prioridades y recursos asignados • Comprobar existencia de niveles de seguridad de los equipos. • Comprobar seguridad en aplicaciones tanto en su transferencia como en su uso. • Verificar existencia de políticas de acceso y protección de aplicaciones • Evaluar el software utilizado, verificar su confiabilidad operacional, y funcionalidad de la información que resulte de los procesos • Verificar si los usuarios tienen correctamente asignado el software correspondiente. • Analizar operaciones, funciones de la red. • Analizar existencia de manuales de los sistemas y aplicaciones. • Verificar políticas de mantenimiento características de los equipos. • Verificar planes de contingencia. • Verificar políticas de seguridad para el servidor y el resto de los equipos • Verificar responsabilidad del uso adecuado del equipo.
Sistema de comunicación	• Verificar que sea la topología adecuada para transmisión de los datos • Verificar normas de seguridad en la transmisión de los datos. • Verificar políticas en el uso adecuado de las comunicaciones. • Verificar nivel de respuesta de los sistemas. • Evaluar conocimiento respecto a la administración de los sistemas de comunicación.
Instalaciones	• Verificar la existencia de normas de seguridad relativas a su mantenimiento • Revisar plan de contingencias ante hechos de riesgo en que sea necesario evacuar el edificio. • Verificar estado, seguridad y distribución de las instalaciones eléctricas en red fija. • Verificar estado en que se encuentra el edificio. • Revisar políticas de mantenimiento de las instalaciones.
Recurso Humano	• Comprobar cumplimiento de las políticas de la empresa • Identificar el nivel de desempeño de la labor realizada • Verificación del nivel de responsabilidad del personal de cada departamento, a través de asignación de cargos • Revisar nivel de capacitación y/o estudios del personal. • Constatar políticas en el uso de claves de acceso y de atributos para operadores y usuarios. • Establecer funcionalidades de cada departamento. • Establecer persona responsable de la administración de la red.

Tabla 3.7: Puntos a evaluar en la Auditoría

3.2.1.5 Ciclo de seguridad

Llegar a estas instancias en el ámbito de la seguridad informática es ya un gran avance, sin embargo no significa que nuestro sistema ya se encuentre protegido y nuestra labor haya terminado. La seguridad debe estar en constante renovación, se debe realizar una gestión periódica, con el objetivo de identificar nuevas amenazas y vulnerabilidades, además de la verificación de la eficacia de las recomendaciones provistas.

Recordemos la figura 2.1 de la relación Amenaza-Incidente-Impacto. El ciclo de seguridad se inicia con la identificación de las amenazas, que pueden provocar incidentes si explotan las vulnerabilidades que exponen los activos a riesgos de seguridad, lo que puede causar daños en la CIA de la información, causando impactos en el negocio; por ello se busca una solución que implemente medidas de seguridad. Esta solución se muestra en las 4 fases de la estrategia de solución, ver figura 2.2, y posteriormente se evalúan estas medidas y se encuentran nuevas vulnerabilidades. y se comienza de nuevo justo como observamos en la figura 3.2

Como podemos apreciar la seguridad involucra a todo un ciclo de actividades. El éxito de una implementación de seguridad sólo se alcanza al buscar la administración efectiva de todo el ciclo.

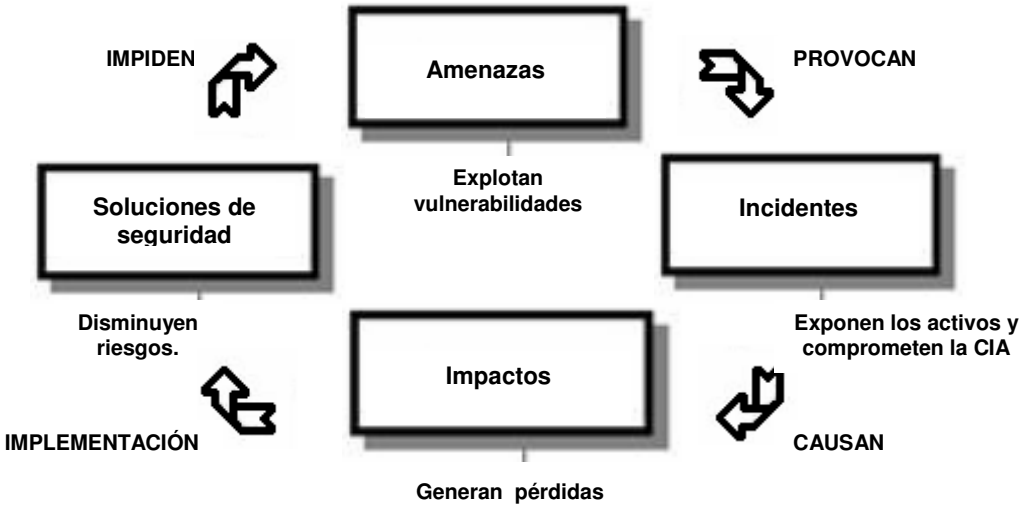
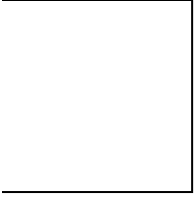


Figura 3.2 Ciclo de seguridad



Capítulo 4

Outsourcing en materia de seguridad de la información

4.1 Panorama del outsourcing

Hoy día las empresas, sean grandes o pequeñas, se enfrentan a la necesidad de ser globales, la necesidad de crecer sin usar más capital, la necesidad de responder a las amenazas y oportunidades de la economía y la reducción de costos. Son muchos los cambios y las necesidades actuales de las empresas, pero también, muchas las alternativas de solución; sin duda, el concepto del outsourcing se escucha cada vez más y ha pasado a formar parte del diálogo de los ejecutivos de las empresas que se orientan a la modernidad operativa que les permita competir bajo reglas avanzadas de compañías globalizadas.

El outsourcing es una práctica que data desde el inicio de la era moderna. Después de la segunda guerra mundial, las empresas trataron de concentrar en sí mismas la mayor cantidad posible de actividades, para no tener que depender de los proveedores. Sin embargo, esta estrategia que en principio resultara efectiva, fue haciéndose obsoleta, ya que nunca los departamentos de una empresa podían mantenerse tan actualizados y competitivos como lo hacían las agencias independientes especializadas en un área.

El objetivo principal del outsourcing es ayudar a las empresas u organizaciones a prever y solucionar conflictos mediante una visión general que permita determinar las prioridades y las principales áreas de oportunidad para mejorar los procesos.

El outsourcing es una estrategia de administración por medio de la cual una empresa transfiere la propiedad y el control de uno o más procesos no críticos a un proveedor altamente especializado para conseguir una mayor efectividad. Así, la empresa deja de realizar una actividad que no forme parte sus actividades principales y puede dedicarse única y exclusivamente a la razón o actividad básica de su negocio, concentrar sus recursos en el negocio principal.

Es preciso aclarar que Outsourcing es diferente de relaciones de negocios y contratación, ya que en éstas últimas el contratista es propietario del proceso y lo controla, es decir, le dice al suplidor qué y cómo quiere que se desempeñen y se fabriquen los productos o servicios comprados por lo que el suplidor no puede variar las instrucciones en ninguna forma. En el caso de Outsourcing el comprador transfiere la propiedad al suplidor, es decir, no instruye al mismo en como desempeñar una tarea sino que se enfoca en la comunicación de qué resultados quiere y le deja al suplidor el proceso de obtenerlos. Además, el outsourcing tiene características diferentes; tiene métricas de constatación contractual, estándares de calidad, servicio al cliente y parámetros de precios.

4.2 El outsourcing como alternativa a la implementación de la seguridad informática para las PyMEs.

El modelo del proveedor externo en el área de tecnología era antes considerado simplemente como un medio para reducir significativamente los costos; sin embargo en los últimos años ha demostrado ser útil para el crecimiento de las empresas. Es una tendencia que se está imponiendo en la comunidad empresarial de todo el mundo y las PyMEs mexicanas no deben quedar fuera ya que se debe tener en claro las condiciones de mercado a las que se enfrenta. El outsourcing para la seguridad en las PyMEs considera que varias empresas utilizan los servicios de una solución de alto costo en forma compartida, sin necesidad de inversión y esfuerzo de instalar uno para si mismas tomando los riesgos que conlleva la limitación de ajustarse a ciertas deficiencias. Así, las empresas ya no asumen la inversión masiva y de golpe, sino que la extienden a lo largo del contrato, beneficiándose con la más reciente tecnología.

La alternativa es que las PyMEs contraten externamente la administración y monitoreo de la seguridad de sus redes y así pueden combinar tecnología avanzada con análisis de expertos, dando como resultado que a la empresa se le garantice una respuesta rápida a las amenazas reales y fortalezca de manera rentable su infraestructura en relación con la seguridad.

4.2.1 Beneficios del Outsourcing

- *Reducción y/o control del gasto de operación.*- Concentración de los negocios y disposición más apropiada de los fondos de capital en funciones relacionadas con la razón de ser de la compañía.
- *Incremento en los puntos fuertes de la empresa.*- Aplicación de los recursos de la organización a las áreas claves.
- *Actualización tecnológica.*- El proveedor asumirá los costos y continuos cambios tecnológicos.
- *Contar con la asesoría de personal altamente capacitado.*- Permite a la empresa tener asesoría de expertos en el área sin la necesidad de entrenar personal de la organización.
- *Mayor eficiencia.*- El manejo de un eficiente nivel de control de calidad del proceso permite a la empresa responder con rapidez a los cambios del entorno; mejora la calidad de la información para las decisiones críticas.
- *Compartir riesgos.*- El proveedor asume las obligaciones legales y fiscales correspondientes. Por sus conocimientos especializados y alta competencia, están obligados a dar resultados a muy corto plazo.

De este modo las PyMEs buscan en un servicio de outsourcing resolver problemas funcionales y/o financieros a través de un enfoque que combina infraestructura tecnológica y recursos humanos en un contrato definido a largo plazo que se ocupe de decisiones de tipo tecnológicos, manejo de proyecto, implantación, administración y operación de la infraestructura.

4.2.2 Características del servicio de outsourcing de seguridad informática

Las empresas deben de adaptarse a través de la experiencia, técnicas, conocimientos específicos y alta competitividad; requiriendo de capacitación y adecuación inmediata de su capital humano para servir de acuerdo a las expectativas, y brindar resultados de manera inmediata. Ver tabla 4.1

Característica	Descripción
Mantener la CIA	Si delega información crítica, debe de firmarse un convenio de confidencialidad y las respectivas penalizaciones por incumplimiento del mismo. El outsourcing debe dar continuidad en caso de desastre. Se debe establecer un acuerdo del alcance y mantenimiento de los niveles de servicio (SLA) y un contrato en el que especifiquen todos los compromisos y responsabilidades de ambas partes. Indicar las penalizaciones por incumplimiento de convenio.
Longevidad	Se invertirá tiempo y recursos para garantizar que el servicio satisfaga las necesidades de la empresa; por tanto, debe ser planeado a largo plazo obteniendo resultado a corto plazo.
Análisis y respuesta en tiempo real	El proveedor debe emplear correlación de sucesos de seguridad y análisis de la información para interpretar con precisión los extensos volúmenes de información sobre seguridad de la red en tiempo real. Debe ser capaz de separar las amenazas reales de seguridad entre una gran cantidad de "falsos positivos".
Instalaciones de última tecnología	Se debe contar tecnología de seguridad de punta: Firewalls, VPN's, IDS y/o IPS, filtros de contenido Web y de correo electrónico. Los cuales garanticen que se cuenta con defensa actualizada contra amenazas, pues constantemente los ataques/virus van siendo más sofisticados.
Expertos en seguridad	Capacitados en los procesos de operación para administrar las herramientas de seguridad, así como monitorear, analizar la información y emitir alertas en tiempo real y recomendar las medidas oportunas que se deben tomar.
Neutralidad del proveedor	Se deben emplear especialistas en seguridad con experiencia certificada en una gran gama de productos entre una variedad de proveedores con el fin de que la compañía tenga la libertad de seleccionar las mejores soluciones de seguridad.
Procesos de administración de la seguridad	Para detectar y administrar vulnerabilidades, desarrollar estrategias y elaborar correlaciones de eventos de seguridad. Debe suministrar normas y políticas documentadas para el correcto control de las operaciones y amenazas. Debe ofrecer una variedad de métodos de notificación de alertas de ataques que permita al personal controlar los riesgos en tiempo real. Definir procesos y procedimientos basados en mejores prácticas para evaluar los incidentes, contenerlos y erradicarlos; procesos para determinar nuevos controles de seguridad, ajustes a la infraestructura o la preparación del personal del cliente.
Informes	Los informes presentados deben ser lo suficientemente detallados para sustentar las decisiones derivadas de las iniciativas de seguridad. Dichos informes detallaran el estado de los dispositivos administrados, las solicitudes de cambio, el desempeño a nivel del servicio, las respuestas sugeridas y la información sobre las últimas amenazas.

Tabla 4.1. Características de un servicio de outsourcing de seguridad

4.3 Servicios de una empresa de outsourcing de seguridad informática.

Objetivos:

- Determinar los riesgos de seguridad de la información en los sistemas de información más críticos y sensibles de una organización.
- Examinar la red de la organización para identificar vulnerabilidades potenciales que pueden ser explotadas.
- Obtener la información necesaria para soportar la parte técnica de la valoración por medio de entrevistas a miembros clave de la compañía.
- Realizar una valoración técnica de la vulnerabilidad de los controles de seguridad en sistemas con información sensible, tales como contraseñas débiles, configuración pobre de los sistemas o prácticas peligrosas para la seguridad que se aplican en el sistema de computación de una organización.
- Eliminar vulnerabilidades basado en las prioridades de la organización.

La tarea de implementar un sistema de seguridad es compleja y requiere los servicios de expertos en la materia. El outsourcing se encarga de la realización de las cuatro fases de la estrategia de solución para la seguridad; de este modo, las PyMEs obtienen un servicio completo en cuestión de monitoreo y administración de la infraestructura dedicada a la seguridad sin tener que invertir en nuevas herramientas, personal o capacitación. Ver tabla 4.2

4.3.1 SOC (Security operation center)

Los centros de operaciones de seguridad (SOC) son estaciones de monitoreo y operación permanente (24 horas al día, 7 días a la semana los 365 días del año) lo que garantiza el constante cumplimiento de las normas de seguridad, altos niveles de servicio manteniendo la seguridad de la información y determinando los ajustes de configuración que se harán en la infraestructura tecnológica.

El SOC detecta, analiza, maneja y erradica, en tiempo real, las amenazas o ataques a la infraestructura o a la información. Permite detectar fallas en cualquier herramienta de seguridad antes de que pueda ser explotada y reparar la vulnerabilidad ya sea de manera remota o informando, con instrucciones claras al cliente sobre qué pasos debe seguir para prevenir cualquier incidente de seguridad sobre su infraestructura o prevenir la sobrecarga de alguna herramienta o activarla nuevamente. El SOC debe cumplir con todas las características de la tabla 4.1.

El SOC monitorea y administra los diversos elementos de la infraestructura encargada de seguridad; esto es, cualquier tipo de acceso y/o actividad que intente evadir los sistemas de seguridad, perjudicar algún sistema, acceder a información sensible o confidencial puede ser detectado inmediatamente y rechazado.

FASE	Resumen	Actividades realizadas por el proveedor externo de seguridad
FASE 1 **Diagnóstico**	El outsourcing se encarga de hacer una minuciosa evaluación del sistema de información, para identificar el grado de vulnerabilidad de la red y valorar el estado actual de su infraestructura de seguridad. Determina los niveles de seguridad del sistema, identifica las zonas desprotegidas y desarrolla las estrategias para corregir situaciones desfavorables. Para conocer el grado de vulnerabilidad del sistema, es preciso examinar el comportamiento de los tres factores básicos de la seguridad: la infraestructura tecnología, los procedimientos y el personal que la opera y monitorea. Se utilizan scanners, analizadores de protocolos, analizadores de vulnerabilidades, programas para la creación de paquetes TCP/IP, exploits, scripts que permiten realizar un barrido de puertos y herramientas de monitoreo, entre otras. El análisis de vulnerabilidades en el personal y la revisión de procesos y procedimientos, se realiza por medio de la valoración del desempeño del personal encargado de la seguridad; para ello se hacen entrevistas de personal, visitas de campo y revisiones de documentos.	▪ Evaluación completa de las tareas que la empresa realiza en red, para definir el tipo de seguridad que más le conviene. ▪ Realizar una valoración técnica de la vulnerabilidad de los controles de seguridad que se aplican en el sistema de computación de una organización; por ejemplo, contraseñas débiles, configuración pobre de los sistemas o prácticas peligrosas para la seguridad. ▪ Detallar las acciones correctivas y elaborar un plan, paso por paso, por prioridades para implementar dichas acciones. ▪ Valorar los riesgos de seguridad de la información en los sistemas de información más críticos y sensibles de una organización ▪ Establecer junto al cliente las partes de su TI que requieren de monitoreo. ▪ Verificar que la compañía cuente con las capacidades necesarias de detección y notificación de incidentes para proteger los sistemas de información crítica o sensible con detectores de intrusos basado en host. ▪ Identificar los segmentos de red que son blancos probables de intrusiones no autorizadas para la protección IDS basada en red.
FASE 2 **Análisis y Diseño**	Se definen las políticas de seguridad de la empresa y se crea la arquitectura tecnológica de seguridad que permitirá resolver las fallas y lograr las mejoras propuestas. Se desarrolla una estrategia y un plan táctico que se ajuste a los requerimientos reales y a los principales objetivos de seguridad y de tecnología de la información de cada compañía.	▪ Optimizar los parámetros de configuración de los sistemas para proteger las aplicaciones y operaciones claves de la empresa ▪ Preparar el entorno informático del cliente para que permita la administración remota y el monitoreo de los sistemas. ▪ Desarrollar políticas y procesos específicos para sus clientes permitiendo que manejen favorablemente cualquier incidente.
FASE 3 **Implantación**	Establecer mecanismos de seguridad que permitan acelerar la respuesta ante amenazas reales. Esto sólo es posible si todas las herramientas se encuentran integradas con el fin de proteger y permitir reaccionar adecuadamente antes amenazas de seguridad. Es necesario integrar procesos de seguridad a la arquitectura tecnológica.	▪ Implementar controles de seguridad para dar seguimiento a los cambios y amenazas a los sistemas clave. ▪ Proporcionar el nivel de respuesta necesario para los incidentes. Diseñar e implementar una capacidad de respuesta centralizada y eficaz.

Tabla 4.2 Estrategia de solución de seguridad implementada por un outsourcing de seguridad.

FASE	Resumen	Actividades realizadas por el proveedor externo de seguridad
FASE 4 **Administración**	Una vez que se diseñó la arquitectura tecnológica de seguridad y que los dispositivos apropiados se instalaron en los lugares más vulnerables, es necesario el monitoreo de las operaciones y en el manejo de la información. Se determina el perfil que deberá cubrir el personal encargado de la seguridad; también se establecen los procesos de administración y monitoreo de la infraestructura tecnológica; también se determinan las acciones a seguir una vez identificado positivamente un incidente de seguridad (recuperar y hacer un seguimiento). Documentar lo sucedido y reducir la posibilidad de repetición de incidentes. Definir los procedimientos de recuperación de los sistemas que pudiesen dañarse debido a un incidente de seguridad. Dar continuidad a esfuerzos proactivos de seguridad de la información tales como el mantenimiento de los lineamientos de seguridad, la actualización del conocimiento de nuevas amenazas y vulnerabilidades, la revisión de las herramientas de soporte para la detección de intrusos. Se realizan auditorías programadas que garanticen la continuidad en el cumplimiento de las políticas de seguridad de la información establecidas por la empresa, y las capacidades de respuesta a incidentes.	▪ Detectar actividades indeseables e intentos de acceso no autorizados. ▪ Identificar y clasificar por categorías los eventos para que el personal pueda reconocer los verdaderos incidentes de seguridad y tomar los pasos para contener y erradicar la amenaza. ▪ Realizar entrenamientos para suministrar al equipo de seguridad una visión general sobre cómo responder a una gran cantidad de incidentes y detalles sobre la preparación que el equipo debe tener para los distintos incidentes de seguridad. ▪ Suministrar un programa de respuesta a incidentes completo y funcional, adaptado bajo la supervisión del cliente, dirigido a los requerimientos específicos de la organización. ▪ Establecer un plan de comunicación de respuesta a incidentes, que incluye la notificación, del tipo de incidente y su impacto potencial en el negocio, a los miembros del equipo, la administración y otras entidades, si es necesario. Definir la manera más apropiada y efectiva de notificación: teléfono, fax o correo electrónico. ▪ Detectar, responder y recuperarse de incidentes. Así como realizar una investigación forense sobre un incidente crítico. ▪ Desarrollar nuevos planes, como el plan de contingencia, el plan de recuperación de desastres y el plan de Continuidad. Para la recuperación de datos perdidos y restauración de la productividad. ▪ Entregar un informe detallado del estado general de los sistemas: áreas que no cumplen y lineamientos para que esos sistemas se apeguen a las políticas. Así como informes sobre las actividades que se realizaron como respuesta a los eventos de seguridad. ▪ Entregar un análisis periódico sobre tendencias que ayuden a determinar si la seguridad está empeorando o mejorando, y cuáles son las razones.

Tabla 4.2 Estrategia de solución de seguridad implementada por un outsourcing de seguridad (continuación)

4.3.1.1 Modelo de arquitecturas.

La definición de arquitecturas fue creada con base en tres dimensiones:

A) Arquitectura tecnológica.

Soporta las funciones operativas del SOC. Indican desde las características físicas (instalación eléctrica, dimensiones, muebles y accesorios), hasta la infraestructura necesaria para soportar el servicio.

Deben implementarse controles de seguridad automatizados, que puedan dar seguimiento a los cambios y amenazas a los sistemas claves de información. Preparar el entorno informático del cliente para que permita la administración remota y el monitoreo de los sistemas seleccionados.

- *Montaje de equipos y mobiliario.*- Diagrama de ubicación e instalación de racks, gabinetes, equipo de cómputo y telecomunicaciones para la infraestructura interna del SOC.
- *Seguridad física.*- Puertas con su respectivo control de acceso al área operativa del SOC.
- *Instalación de hardware y software.*- Instalación y configuración del hardware y software que soportará las funciones operativas del SOC .
- *Pruebas de verificación.*- Criterios que se seguirán para la validación:
    a) Pruebas de conectividad que garanticen la visibilidad de los equipos y el funcionamiento de sus servicios/procesos.
    b) Validación del funcionamiento de las consolas destinadas a la ejecución de actividades de administración y monitoreo.

En la tabla 4.3 vemos algunas soluciones tecnológicas usadas por el SOC.

Solución	Descripción	Beneficio	Observación
Control de Acceso a la Red (NAC)	Administra el acceso a la red mediante políticas de acceso definidas.	Mantener control de los usuarios antes y después de acceder a la red.	Permite la remediación de vulnerabilidades de los sistemas monitoreados.
Protección Inalámbrica	Monitorea, detecta y bloquea accesos inalámbricos no permitidos.	Mantener aislada y protegida la red inalámbrica corporativa.	Las políticas de seguridad se almacenan y se utilizan para distribuirlas a los accesos registrados.
Monitoreo de Dispositivos de Seguridad	Permite el monitoreo en línea de los componentes de la solución de seguridad.	Mantener una visión general respecto a la disponibilidad de los dispositivos que conforman la solución de seguridad.	Permite la generación de distintos reportes para validar el rendimiento de los dispositivos.
Correlacionador de Eventos de Seguridad	Solución de administración de seguridad que almacena y analiza eventos generados en la red.	Esta solución permite detectar, administrar y mitigar amenazas, riesgos y vulnerabilidades detectadas.	Instalación de agentes en los dispositivos se recolectan eventos en una base de datos en donde se realiza la correlación.
Administración de FW / IPS	Bloquean la actividad que no sea válida.	Monitorear, detectar y bloquear actividad sospechosa en la red.	Administración de las reglas para permitir o denegar conexiones.

Tabla 4.3. Tecnologías usadas por el SOC

B) Arquitectura de procesos.

Integrada por los procesos que soportan la operación del SOC. La definición de los mismos debe ser realizada con base en las mejores prácticas de la industria en diferentes ámbitos. De manera continua aportar mejoras a los procesos y procedimientos operativos, y conformar así una estructura de procesos robusta y actualizada.

La tabla 4.4 señala los cuatro procesos generales a cubrir durante la operación diaria:

Proceso	Descripción
Monitoreo de seguridad	En este proceso se monitorea en tiempo real el comportamiento y eventos de la infraestructura de seguridad. Vigila para minimizar y evitar la ocurrencia de amenazas o nuevas vulnerabilidades. Con estas funciones garantizará la operación permanente de la infraestructura de seguridad con el fin de comprobar: ▪ Los niveles de disponibilidad y desempeño. ▪ La existencia de fallas y de actividades sospechosas que pudieran comprometer la seguridad. ▪ El cumplimiento de los lineamientos establecidos en el hardening de la infraestructura monitoreada y administrada por el SOC. ▪ Las reglas, políticas de configuraciones y la ubicación de los dispositivos y controles de seguridad.
Operación (Control de cambios)	Administra y coordina los cambios a la infraestructura. El SOC será el responsable por todos los controles de cambio (emisión, recepción, validación, ejecución y supervisión) efectuados a la infraestructura de seguridad. Toda modificación solicitada por el cliente será responsabilidad del solicitante. Si a juicio del SOC no se recomienda la modificación, su personal se limitará a validar y personalizar las adecuaciones, pero la autorización y responsabilidad final será del cliente. El procedimiento que soporta está función es el de control de cambios y configuraciones.
Soporte (Manejo de incidentes)	En este proceso se encuentra la clave para poder obtener un nivel de seguridad adecuado, ya que define la líneas de acción a seguir al momento en que una actividad sospechosa deriva en un incidente de seguridad. El SOC será capaz de realizar las acciones para llevar a cabo la recuperación de un servicio en la infraestructura administrada, así como también podrá identificar la causa raíz de la falla para dar solución a la misma. Entrega del reporte con los resultados de las actividades realizadas. Los procedimientos que soportan esta función son el procedimiento de manejo de incidentes, el procedimiento de eventos de soporte y el plan de contingencia y/o continuidad.
Administración de niveles de servicio	Mediante esta función el SOC podrá vigilar el cumplimiento de acuerdo a los SLAs establecidos que satisfagan las necesidades operativas. Todos los procedimientos deberán estar apegados a los SLAs.

Tabla 4.4. Arquitectura de procesos

C) Arquitectura organizacional.

Debido al alto grado de especialización en cada una de las áreas que integran la estructura organizacional del SOC. La definición de perfiles y la capacitación del personal, es un proceso complejo que se realiza constantemente. Ver tabla 4.5

Puesto	Descripción	Funciones principales
Ingeniero de operación 1er. Nivel	Monitorea que la solución de seguridad implantada este funcionando de acuerdo a la metodología y notifica en caso de que la operación esté siendo sujeta de ataques que puedan afectar los servicios protegidos y/o la operación de la infraestructura. Dan solución y seguimiento a los eventos de seguridad, llevan a cabo las pruebas necesarias para la validación del mismo.	▪ Operador de consolas de monitoreo. Diagnosticar y solucionar fallas ▪ Generación de reportes y apoyo en la generación de información. ▪ Verificar que los servicios de monitoreo funcionen correctamente. ▪ Generar satisfacción en el servicio a los usuarios, mediante el cumplimiento de las normas, estándares, procesos, políticas, procedimientos, etc. En tiempo y forma de los servicios acordados.
Ingeniero QA (Quality adminitrator) 2do. Nivel	Rol encargado de dar seguimiento a todos los eventos que ocurran. Supervisa y coordina las actividades realizadas por los ingenieros de operación del SOC para la definición e implantación de estrategias de solución. Verifica el apego a los procesos definidos.	▪ Dar soluciones funcionales a problemas más complejos. ▪ Mantener la continuidad de la operación del SOC ▪ Asegurar la calidad de operación de las herramientas de monitoreo. ▪ Maximizar el uso de herramientas, procesos y metodologías..
Analista 3er. Nivel	Es el líder técnico del SOC. Lleva a cabo la toma de decisiones en caso de identificar que la operación está siendo sujeta de un ataque. Analiza la información en conjunto con el TAM ante eventos de alto impacto. Es el responsable de procesos de monitoreo, de administración de incidentes y de administración de cambios y configuraciones.	▪ Vigilar el cumplimiento del modelo operativo definido ▪ Vigilar el apego a los procesos y procedimientos definidos ▪ Planea la estrategia a llevar a cabo. Realiza adecuaciones a la metodología operativa en caso de ser necesario ▪ Brindar asesorías, sobre la ejecución de un proceso de operación ▪ Redefinir los procedimientos de atención del SOC con el cliente.
IRT (Incident Respond Team) 4to. Nivel	Realizar las acciones necesarias para la contención de un incidente y el análisis forense del mismo en caso de que ocasione daño. Este equipo está formado por personal capacitado y con experiencia en el monitoreo y repuesta a ataques de seguridad informáticos.	▪ Último nivel técnico de escalación interna en el SOC. ▪ Responsable del proceso de administración de problemas ▪ Coordinación de las acciones a realizar antes, durante y después de presentarse un incidente de seguridad
Tigre Team	Equipo que se encarga de realizar pruebas de penetración, emitir alertas de nuevas vulnerabilidades	▪ Monitoreo permanente de virus, ataques y vulnerabilidades. ▪ Investiga parches y envío de alertas para minimización del impacto.
Gerente del SOC	Rol encargado de dar seguimiento a todos los eventos que ocurran, verifica el apego a los procesos definidos, es el encargado de dar el Vo. Bo. de aquellas solicitudes que sea necesario escalar.	▪ Disponibilidad para ser contactado a cualquier hora del día y noche ▪ Toma de decisiones en eventos críticos ▪ Solución a eventos orientado al cumplimiento de SLA's
TAM (Tecnical Account Manager)	Da seguimiento a los clientes, mantiene una estrecha relación con ellos para asegurar que todos sus requerimientos son atendidos de manera adecuada y que corresponde con los niveles acordados.	▪ Tomar decisiones de emergencia ante eventos de alto impacto. ▪ Negociaciones y seguimiento a pendientes con las cuentas del SOC ▪ Receptor de la percepción del servicio que se proporciona al cliente.
Director del SOC	Encargado de liderar y dar apoyo en eventos de alta prioridad, es decir, aquellos que puedan resultar en daños o pérdidas graves a la información o infraestructura.	▪ Llevar a cabo la toma de decisiones ante eventos de mayor impacto y que puedan resultar en sanciones por incumplimiento

Tabla 4.5 Descripción de los roles dentro del SOC

4.3.1.2 Interacción Cliente-SOC

En caso de ocurrir algún evento de seguridad es indispensable garantizar, a través de la definición de los canales de comunicación y actividades para la recepción, solución, seguimiento y cierre de eventos, la atención oportuna de los requerimientos o incidentes de seguridad; entendiendo por atención oportuna al cumplimiento de los tiempos definidos en los niveles de servicios.

El cliente notifica por teléfono o vía correo al SOC, se analiza la solicitud y si existe algún problema se pasa el reporte al siguiente nivel de atención, donde se resuelve cancelando, modificando o aceptando el requerimiento. Ya sin problemas por resolver, se realiza lo necesario para poner en práctica el requerimiento. Se notifica al cliente del cambio y se pide su validación, de ser validada, se documenta y cierra el reporte, en caso contrario, se comienza de nuevo el ciclo. En el diagrama 4.1 vemos el flujo de comunicación.

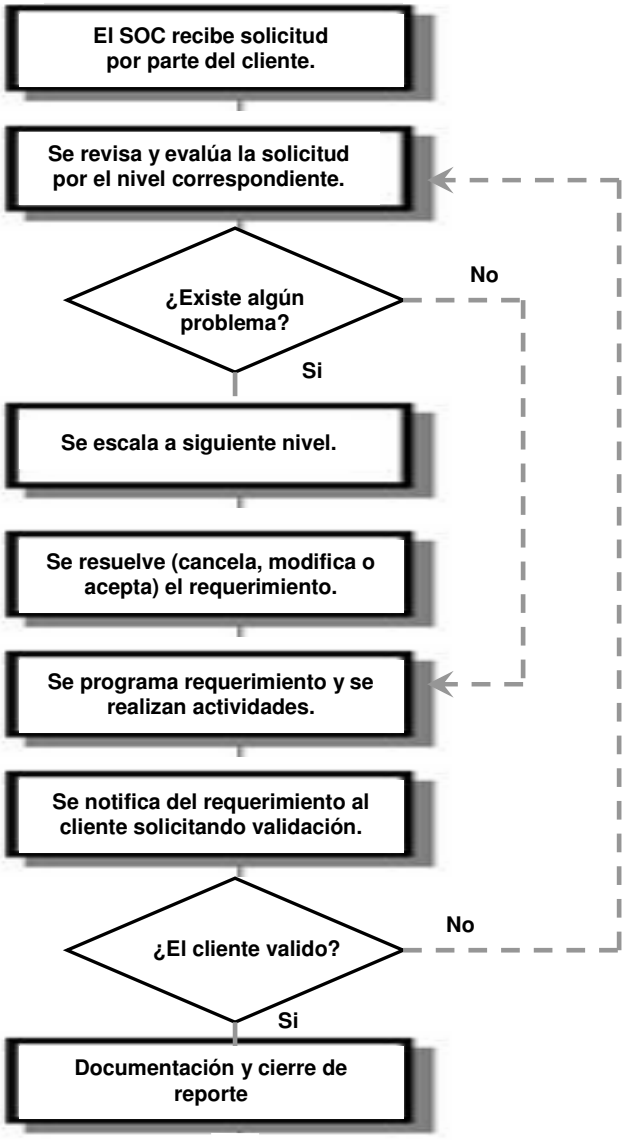


Figura 4.1 Diagrama de flujo de la interacción Cliente-SOC

4.3.2 Definir procedimientos de seguridad

La finalidad es que ante la ocurrencia de un incidente de seguridad, se recupere y/o normalice la operación lo más pronto posible y se minimice el impacto que pueda ocasionar en el cumplimiento de los objetivos de negocio, garantizando que los niveles de calidad y disponibilidad del servicio sean mantenidos implementando y siguiendo a ciertos controles que disminuyan el riesgo residual a un nivel aceptable.

Existen gran número de procedimientos siendo los más importantes los que a continuación se muestran; están basados en las mejores prácticas y recomendaciones efectivas para la administración de servicios de seguridad de la información. Están conformados por un conjunto de estándares desarrollados por profesionales líderes en el ramo con el fin de reducir los costos y al mismo tiempo mantener el nivel de los servicios.

1. Procedimiento de eventos de soporte
Su objetivo es que ante la ocurrencia de una falla imprevista en la operación de la infraestructura de seguridad se restaure la operación normal de los servicios tan pronto como sea posible, cumpliendo siempre con los tiempos de atención definidos en los SLA's, y minimizar el impacto en el negocio.

2. Procedimiento de control de cambios y configuraciones
El objetivo es describir de manera clara y puntual el proceso de control de cambios en la resolución de eventos de soporte, mantenimiento y actualizaciones que requieran la aplicación de los mismos, con el fin de asegurar que todos los cambios sean controlados.

3. Proceso de manejo de incidentes
Tiene como objetivo el definir el conjunto de acciones que nos permitan recuperar o normalizar la operación lo más pronto posible minimizando el impacto ocasionado por cualquier incidente de seguridad, garantizando que los niveles de calidad y disponibilidad del servicio sean mantenidos

4. Plan de contingencia y/o continuidad
Entre sus principales objetivos se encuentran:
- Asegurar la capacidad de supervivencia de la compañía
- Garantizar la continuidad de las operaciones de la empresa, no sólo de sus sistemas de información.
- Reducir la probabilidad de las pérdidas, a un nivel mínimo aceptable, a un costo razonable y asegurar la adecuada recuperación.
- Asegurar que existan controles adecuados para reducir el riesgo por fallas tanto del equipo, software, datos y medios de almacenamiento.

4.3.2.1 Procedimiento de eventos de soporte

Entradas:
Lo que dispara el inicio de las actividades del procedimiento:
- Reporte de apertura. (Descripción del evento)

Salidas:
A través de la ejecución de este proceso, el SOC deberá obtener:
- Análisis del evento (Causas, líneas de acción)
- Reporte de cierre. (Validación, prevención de evento, periodo de monitoreo)

Descripción de las fases:
La tabla 4.6 muestra las fases de este procedimiento.

Fase	Descripción
Detección	Identificación de eventos que puedan afectar o comprometer la disponibilidad de los servicios u operación de los dispositivos; pueden ser originados por: ▪ El cliente.- Se identifica algún tipo de problema de soporte, falla o interrupción en los servicios o dispositivos y se genera un reporte. ▪ El SOC.- A través de sus herramientas de monitoreo identifica: actividades sospechosas, incidentes y fallas.
Recepción de eventos	La recepción de eventos de soporte en el SOC se realizará a la línea telefónica de atención al cliente o vía correo electrónico. Se recibe la notificación y se documentará la descripción del evento recibido en el formato correspondiente.
Análisis y Programación del Evento	Analizar y definir la programación para la solución del incidente. Señalar: ▪ Origen o causas que pudieron dar origen al evento. ▪ Solución: Inmediata o planeada. Depende de la prioridad del evento. ▪ Definición de las líneas de acción a seguir. ▪ ¿Es necesario que alguien apoye en sitio (instalaciones del cliente)? ▪ ¿Es necesario reemplazar alguna pieza del equipo?
Ejecutar acciones	Esta fase da la entrada para el proceso de control de cambios, ya que en éste se realiza el diseño del plan de implantación del cambio a seguir.
Seguimiento Y Control	Se realizan las pruebas y acciones de prevención que minimicen la recurrencia de la misma falla. Si depende de un proveedor externo o si la falla corresponde a un dispositivo físico, es responsabilidad del SOC el seguimiento, así como de informar el estatus actualizado de los eventos al cliente.
Validación de la solución	La solución deberá ser validada tanto por el cliente como por el SOC. El registro de la validación debe estar dentro de la documentación.
Cierre del Evento	En el caso de que por su complejidad o su impacto con el resto de la operación necesite un periodo determinado de monitoreo, éste debe ser especificado en el mismo formato de cierre del evento. Al terminar dichos los periodos de monitoreo de un evento, éste debe ser validado nuevamente.

Tabla 4.6. Fases del procedimiento de eventos de soporte

4.3.2.2 Procedimiento de control de cambios y configuraciones

Entradas:
El origen de un cambio puede tener los siguientes orígenes:
- Modificación en la arquitectura de seguridad. Fallas en software y hardware
- Solución a un evento de soporte de áreas internas o directamente del cliente
- Vulnerabilidades detectadas por el proceso de administración.
- Actualizaciones para en la configuración de las aplicaciones

Salidas:
El procedimiento de control de cambios generará:
- Análisis de viabilidad de aplicación de cambios
- Plan de implantación y Plan de contingencia del cambio

Descripción de las fases:
El diagrama 4.2 muestra el flujo del procedimiento y la tabla 4.7 un resumen de sus fases.

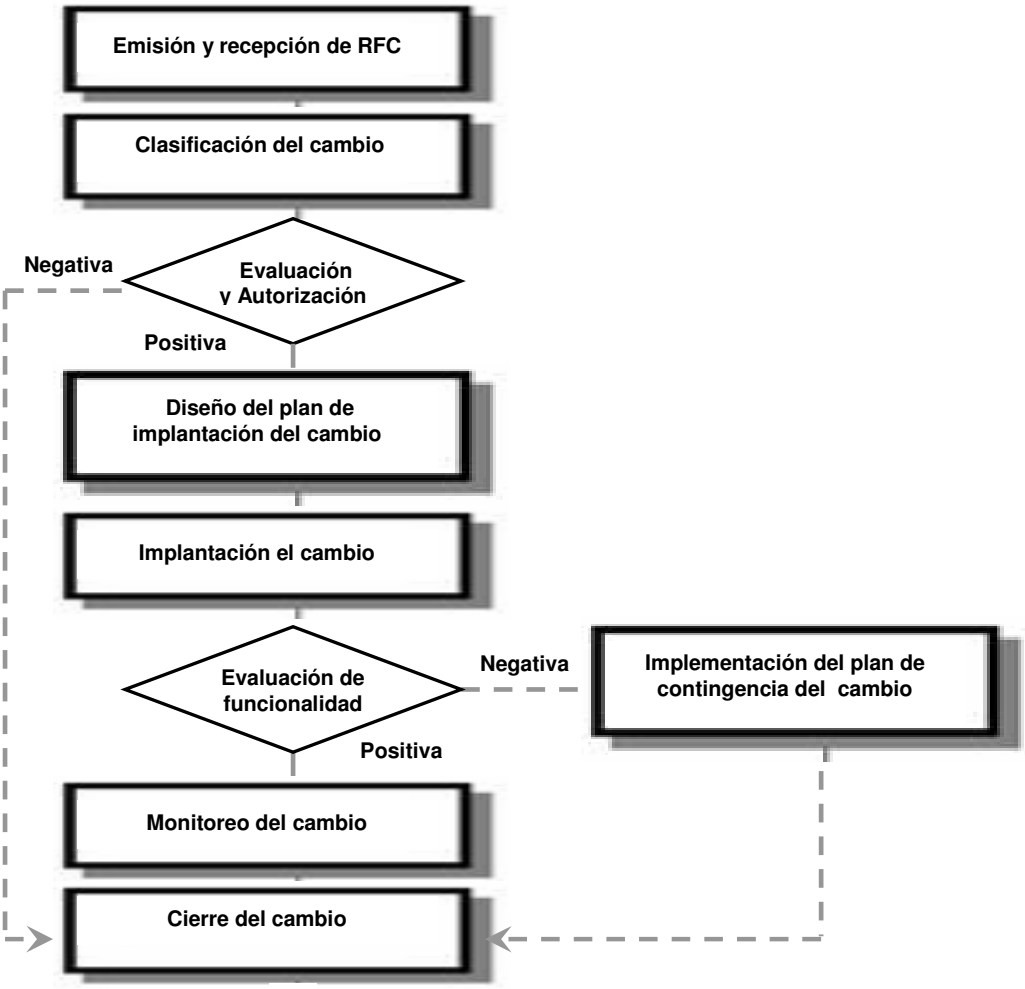


Figura 4.2 Diagrama de flujo del control de cambios y configuraciones

Pasos	Descripción
Emisión y Recepción del RFC	Se refiere a una petición de cambio, RFC (Request for change), en alguna parte de la infraestructura, ya sea un cambio físico en un equipo o cambio en la configuración de un componente en nuestra TI. Un RFC puede ser solicitado directamente por el cliente o bien, puede derivarse de un error encontrado como resultado de la interacción con los procesos de respuesta a incidentes, operación y monitoreo o administración de vulnerabilidades.
Clasificación del cambio	Después de recibir el RFC se verifica el tipo de cambio a realizar, por ej.: requerimiento de cambio del alcance del proyecto, requerimiento de validación de cambio, requerimiento de cambio de la infraestructura.
Evaluación y Autorización	Dependiendo de su impacto y magnitud, el cambio deberá de ser analizado y autorizado por el (los) nivel(es) correspondiente(s). El resultado de esta decisión, definirá la continuación o término de las siguientes fases del proceso. En caso de que el resultado sea negativo, el cambio no debe de aplicarse, es decir, no llevar a cabo la implantación del cambio, a causa de los riesgos en la operación y la probable exposición a vulnerabilidades; se cerrará el proceso con el cierre del mismo y la justificación bajo la cual se tomó la decisión correspondiente. En caso de que el resultado sea positivo, se continuará con la aplicación de las siguientes fases del proceso.
Diseño del plan de implantación del cambio	Se define el diseño para la implantación y monitoreo para evaluar el comportamiento del cambio después de su aplicación; involucra, recursos, actividades, horarios e identificación de servicios directamente afectados. Así también debe de incluir las actividades a realizar en caso de que al llevar a cabo la implantación del cambio se presenten problemas inesperados que afecten a la operación, es decir la definición del plan de contingencia para el cambio que permitirá regresar la configuración afectada a la última en funcionamiento adecuado.
Implementación del cambio	Se realizan las acciones necesarias para la implantación del cambio, éstas deben llevarse a cabo con base en el plan definido. Todos los cambios que se realicen deben ser documentados y contener la siguiente información. ▪ Descripción del cambio (Complejidad e impacto) ▪ Cambio permanente o temporal ▪ Sección de autorizaciones internas ▪ Descripción de las pruebas a realizar y del plan de contingencia ▪ Detalle de actividades de ejecución durante la implantación del cambio ▪ Resultado de los cambios aplicados
Evaluación de la funcionalidad	Se llevan a cabo las acciones necesarias para evaluar el impacto de la aplicación del cambio en la infraestructura directamente afectada, así como en los servicios y aplicaciones que interactúan directamente con él. Esto permitirá identificar aquellos puntos en los que el funcionamiento de la operación no sea el adecuado o él que se espera y se validará la necesidad de llevar a cabo la aplicación del plan de contingencia para el cambio o no.
Plan de contingencia para el cambio	Esta medida permite regresar al funcionamiento adecuado de la operación si existe alguna falla. Si no existe ningún problema con la funcionalidad se continúa a la siguiente fase.
Monitoreo del cambio	Se lleva a cabo el monitoreo del cambio por un periodo de tiempo determinado, para identificar cualquier anomalía o actividad irregular en la operación. Esta actividad se debe llevar a cabo aún después de haber determinado la evaluación exitosa de la funcionalidad.
Cierre del cambio	Última fase, durante la cual se obtienen las validaciones internas (SOC) y externas (cliente) de que el cambio fue realizado exitosamente, dando como resultado la documentación con la descripción completa.

Tabla 4.7. Fases del procedimiento de control de cambios y configuraciones

La tabla 4.8 nos muestra algunos de los tipos de cambio que pueden llegar a presentarse.

Tipo de cambio	Riesgos	C / I	Consideraciones
Agregar una regla en el Firewall	Puede afectar a la operación si la regla agregada no se ubica en el sitio adecuado dentro de la tabla de reglas. Si la regla compromete la seguridad, hacer conciente al cliente sobre el riesgo	**Medio / Alto**	▪ Hacer una revisión de las reglas ya hechas. ▪ Realizar una verificación antes de aplicar políticas. ▪ Generar un respaldo antes de hacer el cambio, dependiendo de la complejidad que implique.
Modificar una regla en el Firewall	La modificación de parámetros de configuración puede afectar la disponibilidad de servicios e incluso dejar canales de comunicación abiertos.	**Medio / Alto**	▪ Realizar un respaldo antes de hacer el cambio. ▪ Revisar el orden de precedencia de las políticas ya hechas. ▪ Aplicar políticas en el Firewall para que tenga efecto el cambio.
Modificar o agregar usuarios en el Firewall	Altas, bajas y cambios de usuarios en el Firewall y de usuarios remotos VPN. No afecta directamente en la operación.	**Baja / Baja**	▪ Aplicar políticas en caso de que este usuario este activo en una regla. ▪ Llevar un registro de usuarios ▪ Generar contraseñas de manera aleatoria.
Agregar o cambiar rutas en los dispositivos de red	Puede afectar directamente a la operación ya que implica hacer modificaciones en la parte de comunicaciones entre dispositivos y ruteo.	**Alto / Alto**	▪ Realizar respaldo de la configuración antes de realizar cualquier cambio. ▪ Revisar las rutas que se van a agregar. ▪ Revisión de los SLAS para saber cuanto tiempo tenemos para realizar el cambio.
Modificar o aplicar políticas a los sensores del IDS	Realizar un análisis previo de las políticas que serán aplicadas a un sensor, para no afectar servicios críticos, ya que si esta actividad no es supervisada se corre el riesgo de afectar la disponibilidad para la operación del cliente.	**Alto / Alto**	▪ El análisis debe considerar la ubicación (ya sea de red o de host) importancia y criticidad de los equipos (DMZ, interno, externo) ▪ Realizar respaldo de la política que se encuentra en producción. ▪ Realizar el análisis previo junto con el cliente antes de la nueva política.
Actualizar los IDS	De no realizarse puede impactar en un futuro, ya que las firmas no se actualizan con las nuevas versiones.	**Medio / Medio**	▪ Llevar un registro de las actualizaciones realizadas. ▪ Realizar los cambios en ventanas de mantenimiento programadas.
Accesos a sitios Web.	Bloquear o permitir accesos a determinados sitios Web.	**Baja / Medio**	▪ Documentar e identificar el o los sitios web, así como a los usuarios afectados

Tabla 4.8 Ejemplos de algunos requerimientos de cambio

4.3.2.3 Proceso de manejo de incidentes

Entradas:
Lo que da inicio a este proceso es la ocurrencia de cualquier evento que amenace la seguridad en los sistemas de información.

Salidas:
A través de la ejecución de este proceso, se deberán obtener los siguientes resultados:

- Reporte de la identificación y registro del incidente.
- Registro de las acciones realizadas, para la contención y seguimiento del incidente
- Reporte forense (en caso de que aplique).

Descripción de las fases:
En el diagrama 4.3 vemos el flujo de las fases del proceso y en la tabla 4.9 tenemos un resumen de en qué consiste cada uno de los procedimientos que forma cada fase.

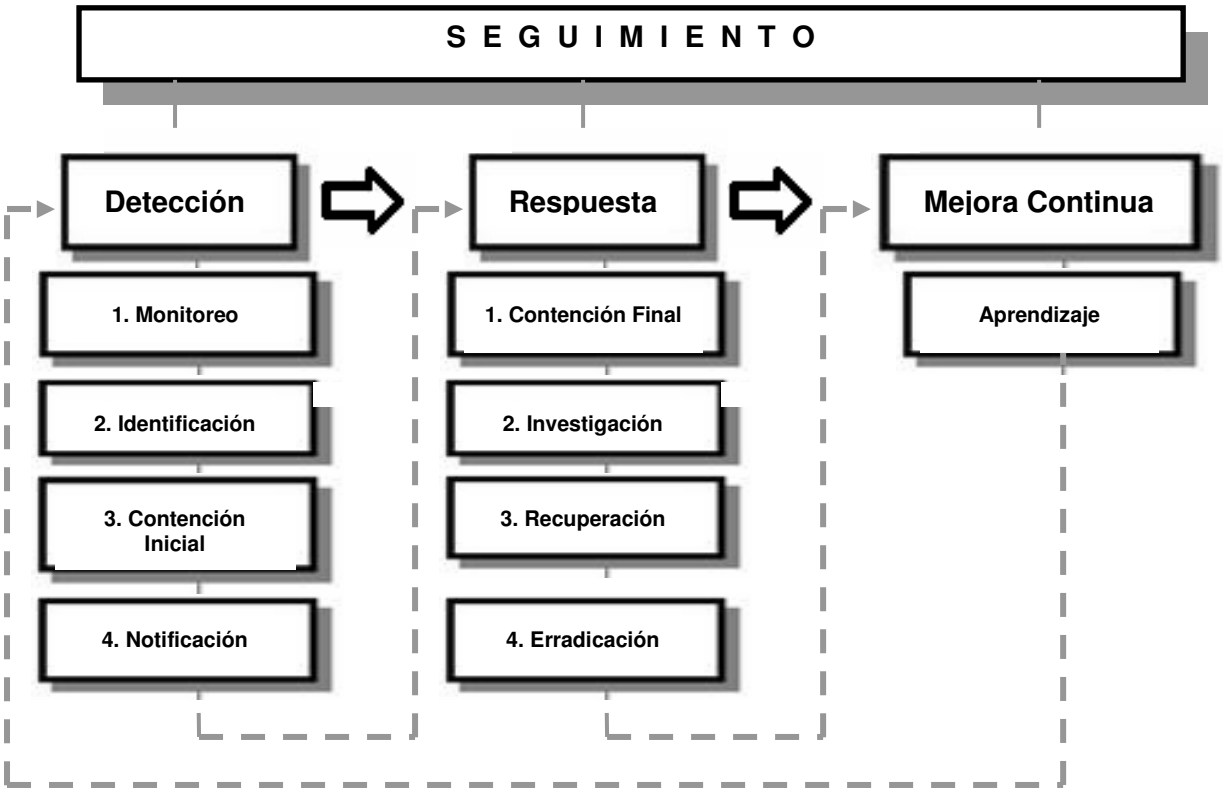


Figura 4.3 Diagrama de flujo del procedimiento de Manejo de Incidentes.

Fase	Descripción de la fase	Procedimientos	Descripción del procedimientos
Detección	▪ Ocurre durante el monitoreo. ▪ El ingeniero de operación se da cuenta de algún comportamiento inusual, sospechoso o no esperado. ▪ Se identifica algo que debe ser analizado más a detalle o que el sistema requiere la aplicación de algún cambio ▪ Se notifica a los involucrados para llevar a cabo las acciones de respuesta ▪ Confirmación de las actividades sospechosas sean o no ataques	Monitoreo: I. En línea II. Fuera de línea	▪ Explotación de Bitácoras / Logs ▪ Inspecciones manuales ▪ Detección en línea y detección por generación de Alertas
		Identificación	▪ Confirmación de incidente. Asociación de los eventos detectados ▪ Captura y registro de la información del sistema ▪ Tipificación del incidente a la magnitud, impacto y prioridad.
		Contención Inicial	▪ Análisis de la información y acciones Iniciales de mitigación ▪ Interfaz directa con el proceso de control de cambios
		Notificación I. Tipificaciones II. Confirmación III. Comunicación	▪ Notificación y/o escalamiento al responsable de hacer la contención final y erradicarlo, a través de la matriz de escalamiento. ▪ Notificación a las personas/áreas involucradas ▪ Tipificación de incidentes
Respuesta	▪ Se analizan los efectos, alcances y daños causados por la intrusión. ▪ Se realiza la contención ▪ Se ejecuta líneas de acción para eliminar futuros accesos a intrusos. ▪ Recupera el estado operacional de los servicios. ▪ Verificación de las actividades de acuerdo al patrón de ataque ▪ Identificación de los ataques utilizados para obtener acceso	Contención final	▪ Dependiendo del evento se asocia una secuencia de acciones a ejecutar ▪ Aislamiento de los equipos/sistemas comprometidos ▪ Interfaz directa con los procesos de control de cambios y configuraciones
		Investigación	▪ Revisión de equipos/sistemas en búsqueda de señales de intrusión ▪ Recolección y protección de información. Preservar evidencia ▪ Identificación de las actividades realizadas por el intruso
		Recuperación	▪ Recuperación de la operación, de comunicaciones,datos y configuraciones ▪ Interfaz directa con el proceso de control de cambios y soporte
		Erradicación	▪ Realizar un análisis de vulnerabilidades sobre los equipos afectados. ▪ Ejecutar actividades de aseguramiento para remover la causa del incidente. Interfaz directa con el proceso de control de cambios
Mejora Continua	▪ Ejecución de acciones para fortalecer las plataformas afectadas. ▪ Actualización de políticas, procedimientos y herramientas.	Aprendizaje	▪ Identificación y establecimiento de mecanismos de prevención y control ▪ Mejorar los procesos a través de las lecciones aprendidas ▪ Reunión post-mortem (seguridad forense).
Seguimiento	▪ Continuidad a cada una de las fases que integran el proceso ▪ Solución de eventos por etapas	Registro Escalamiento Cierre	▪ Generación y revisión de las alarmas levantadas (Cambios, requerimientos soporte, etc) ▪ Niveles de Escalamiento.

Tabla 4.9 Fases del procedimiento de manejo de incidente

1. Detección

Esta fase involucra la identificación de patrones de ataques o de actividad inusual que pueda ocasionar daño a la infraestructura de TI.

Garantizar que a través de las actividades permanentes se clasificaran los eventos de seguridad de acuerdo a su gravedad e impacto para identificar la prioridad en la que deben ser resueltos y escalados.

1.1 Monitoreo

Garantizar que los administradores de la infraestructura identifiquen aquellas actividades inusuales que puedan dar origen a fallas en los sistemas, ocasionando interrupción en los servicios que se brindan o afectando la CIA de la información que procesan.

Involucra la revisión permanente de las actividades que se desarrollan en los sistemas, tanto en desempeño como en rendimiento de la infraestructura al soportar la operación diaria. Lleva a cabo el registro de aquellos eventos que comprometan la seguridad.

Es importante identificar la ubicación de los dispositivos que realizaran dichas funciones, para verificar todo el tráfico que viaja a través de ésta, en servidores con aplicaciones, bases de datos o servicios críticos, etc.

El detalle de la información a recolectar para la detección de actividades inusuales en la operación del firewall y de los IDS involucra aspectos relacionados con:

- Desempeño de la red, del sistema y de los procesos
- Archivos y Directorios (Accesos, creación, modificación, ejecución, eliminación, etc.)
- Usuarios (Información de acceso y salida, intentos exitosos o fallidos de accesos a cuentas privilegiadas, etc.)
- Aplicaciones
- Bitácoras
- Vulnerabilidades

Es importante señalar que como parte de la preparación para el inicio del monitoreo, se deben registrar y almacenar las configuraciones originales de los dispositivos, las cuales servirán para llevar a cabo actividades de recuperación en caso de fallas o incidentes y como base de comparación para identificar las modificaciones que puedan sufrir las mismas.

1.2 Identificación

Realizar la comparación de los eventos registrados contra un patrón de incidentes para confirmar la existencia o no de una actividad sospechosa como incidente.

La importancia de este procedimiento radica en evitar:

- El no poder determinar la extensión y daño ocasionado por el incidente.
- La utilización de la infraestructura tecnológica para generar ataques o daños en contra de otros sistemas de otras organizaciones.
- La pérdida de oportunidades de negocio.

En necesario recabar la siguiente información, para dar inicio a las actividades del procedimiento de contención.

- Dispositivos y servicios afectados
- Responsables
- Tipificación del incidente
- Determinación del impacto para definir la prioridad del mismo.
- Registro de la actividad sospechosa en el formato correspondiente

1.3 Notificación

Informar de manera oportuna a clientes, proveedores y entidades directamente afectadas por el incidente.

Con base en la prioridad asociada al incidente, los responsables en la toma de decisiones definirán las actividades para la contención y erradicación.

Escalar los eventos en caso de que el impacto de los ataques o incidentes no se detengan con las actividades de contención inicial y el tiempo transcurrido exceda los límites definidos por la organización.

2. Respuesta

Lograr que el alcance y la magnitud del incidente sean limitados y que la operación normal sea reestablecida, garantizando que la implantación de los controles necesarios sean puestos en marcha para evitar la recurrencia.

2.1 Contención

Limitar el alcance y la magnitud del incidente, evitando cause daños mediante la aplicación de tácticas para detener el acceso del intruso al dispositivo violado, limitar la extensión del incidente y prevenir daños adicionales y futuros que pudiera causar el atacante.

Actividades que se realizan para mitigar el impacto del incidente:

- Aislamiento del equipo o equipos afectados
- Reinició del equipo comprometido o afectado
- Realización de respaldos de emergencia
- Realización de actividades para la recolección de evidencia
- Baja temporal del servidor
- Deshabilitar servicios, accesos y cuentas
- Cambiar contraseñas
- Reinstalar componentes de software

2.2 Recuperación

Verificar que las actividades de contención realizadas apoyen en regresar los servicios a su operación normal.

- Restauración con respaldos en caso de pérdida de información,.
- Restablecer operación en caso de baja de servicios o desconexión de equipos.

2.3 Investigación

Encargarse de llegar a la raíz del incidente, a través de la recolección de evidencia que permita identificar la vulnerabilidad explotada, impacto, etc.

Dentro de las actividades a realizar en este procedimiento se encuentran:
- Captura y registro de la información del sistema
- Recolección de evidencia
- Respaldo de los sistemas comprometidos
- Revisión de bitácoras

Si la información para la identificación y contención (incluso la evidencia) no se recolecta de manera rápida y acertada, puede perderse para siempre.

2.4 Erradicación

Definición de controles de detección, prevención y corrección que eviten la recurrencia de incidentes y eliminen el problema de raíz, a través del análisis del origen del mismo y de los factores utilizados para su explotación, evitando que la operación siga funcionando bajo el riesgo de volver a ser atacado a través de ataques o intrusiones similares.

Dentro de las principales actividades de este procedimiento se encuentran:
- La ejecución de un análisis de vulnerabilidades a los equipos comprometidos, para garantizar que la vulnerabilidad explotada no pueda volver a ser utilizada para fines dañinos.
- Administración de parches y actualizaciones.

3. **Mejora Continua**

Realizar una revisión posterior al evento ocurrido con todas las partes involucradas evaluando los resultados obtenidos en la resolución del incidente, y de ser posible responder en el menor tiempo

3.1. Aprendizaje

Garantizar la eficiencia del proceso ante eventos similares identificando las áreas de oportunidad a partir de las acciones exitosas y fallidas.

Las lecciones aprendidas ayudarán a mejorar el trabajo en el futuro y también a identificar si alguien del equipo no actuó de acuerdo a las políticas y códigos de conducta definidos.

Dentro de las actividades de este procedimiento se encuentran:
- Analizar toda la documentación producida
- Incluir a todas las entidades afectadas en la revisión del reporte
- Elaborar el reporte de lecciones aprendidas. Emitir recomendaciones.
- Validar y crear consenso. Implantar acciones aprobadas.

4. Seguimiento

El objetivo es garantizar el correcto flujo del proceso de manejo de incidentes; apoyar en la ejecución de los procedimientos facilitando y verificando que el proceso avanza de manera óptima y sin contratiempos. En caso que exista un problema, reportarlo y garantizar que se tomen las líneas de acción necesarias para resolverlo.

Se enfoca a evaluar y corregir cualquier anomalía en el desarrollo o aplicación del proceso de manejo de incidentes, tratando de facilitar soluciones y reportar fallas de ejecución, así como el verificar que se cumplan con las políticas y procedimientos establecidos para el desarrollo de las actividades.

4.3.2.4 Plan de contingencia y/o continuidad

A medida que las empresas se han vuelto cada vez más dependientes de la TI para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos. La interrupción prolongada de las operaciones, la pérdida de todos los datos de la empresa o el fallo de equipos vitales del sistema o de los servicios puede llevar a pérdidas financieras significativas. La causa puede ser desde la falta de provisión de servicios tales como energía eléctrica y/o telecomunicaciones, robo o hasta un desastre natural. Si bien un seguro puede cubrir los costos materiales de los activos de una organización en caso de una calamidad, no servirá para recuperar el negocio.

La reanudación de las actividades ante un desastre puede ser una de las situaciones más difíciles con las que una organización deba enfrentarse. La única manera efectiva de afrontar un incidente de tal magnitud es tener una solución completa y totalmente probada para recuperarse de los efectos del mismo. La capacidad para recuperarse exitosamente de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan estratégico de seguridad para una organización.

El diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y gastos considerables. Requerirá del desarrollo y prueba de muchos procedimientos nuevos, y éstos deben ser compatibles con las operaciones existentes. Se hará participar a personal de diferentes departamentos, quienes deberán trabajar en conjunto cuando se desarrolle e implemente la solución. Implicará un compromiso entre costo, velocidad de recuperación, medida de la recuperación y alcance de los desastres cubiertos. Debemos tener presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas.

Descripción de las fases:

1. **Constitución del grupo de desarrollo del plan.**
   Este grupo debe estar liderado por un responsable y formado por los líderes de las áreas que se desean cubrir con dicho plan. La dirección de la empresa debe colaborar íntimamente con el SOC durante todo el proceso.

2. **Identificación de riesgos**
   Definir los posibles escenarios con los que podemos encontrarnos para cada función crítica. Puede tratarse de problemas en:
   - El hardware, software de base, software de aplicación propio o provisto por terceros.
   - La utilización indebida de medios magnéticos de resguardo o cualquier otro daño de origen físico que pudiera provocar pérdida de información.
   - Carencia de fuentes de energía y de telecomunicaciones.

Deben incorporarse todos los componentes del sistema susceptibles de ser dañados, dando lugar a la pérdida de conectividad o datos. Un diagrama de la arquitectura de todos los componentes del sistema facilitará la realización de un inventario de los elementos que pueden necesitar ser restituidos tras un desastre; un error u omisión en el inventario puede dar lugar a una recuperación fallida tras un desastre.

El sistema de aplicación puede no encontrarse preparado para su uso si alguno de sus componentes no está disponible. No debemos olvidar que el software necesita ser identificado y reemplazado; esto incluye cosas como las utilidades del sistema de archivos empleados para facilitar las operaciones de red. Deben considerarse mecanismos alternativos de acceso a la red en el caso de que, por alguna razón, sea imposible acceder al inmueble, incluso aunque el edificio puede estar en pie y operacional.
Los errores humanos son una de las causas más probables de la pérdida o deterioro de los datos. Si un error de este tipo provoca la pérdida de un sistema en la red, tiene el mismo efecto que cualquier otro tipo de desastre, y como tal debe ser tratado.

3. Evaluación del riesgo
Determinar el costo para la organización de sufrir un desastre que afecte su actividad. En el caso de los sistemas informáticos, la preocupación principal es comprender la cantidad de pérdida financiera que puede provocar la interrupción de los servicios, incluyendo los que se basan en las redes.

Los costos de un desastre pueden clasificarse en las siguientes categorías:
- *Costos reales de reemplazar los equipos y el software.*- Es fácil de calcular, y depende de si se dispone de un buen inventario de todos los componentes de la red necesarios.
- *Costos por falta de producción.*- La empresa tiene una valoración de la cantidad de trabajo realizado diariamente y su valor relativo.

Una correcta cuantificación del impacto económico de cada problema ayudará a una correcta selección de la solución alternativa. Las aplicaciones cliente/servidor o distribuidas añaden un nivel extra de complejidad al requerir que distintas partes de la aplicación residan en máquinas separadas.

4. Asignación de prioridades
Identificación de las funciones críticas y jerarquizarlas por orden de importancia dentro de la organización para poder reestablecer los sistemas, satisfacer las necesidades básicas y así poder reanudar las operaciones lo antes posible. Un ejemplo muy sencillo de jerarquización de actividades:
1. Restablecer los servidores donde las aplicaciones almacenan sus datos,

2. Reinstalar el sistema. Software de las aplicaciones y estaciones de trabajo que los procesan, la red que interconecta todo, y las impresoras o faxes empleados para entrada/salida,
3. Restablecer los respaldos y
4. Continuar con la operación.

5. Establecimiento de requisitos de recuperación
El cliente tiene que decidir el periodo predeterminado que lleva una interrupción de servicio de la situación de "problema" a la de "desastre". Se trata de definir los mínimos niveles de servicio aceptables para cada problema que se pueda plantear. Esto se logra llevando a cabo un análisis de impacto en el negocio para determinar el máximo tiempo de interrupción permisible en funciones vitales de sus actividades.
La clave es definir el tiempo de recuperación objetivo (TRO, Recovery Time Objective), periodo de tiempo aceptable y viable para lograr que el negocio esté de nuevo activo; el TRO debe ser verificado para comprobar que es realista y factible.

6. Identificación de las alternativas de solución.
Identificar las soluciones alternativas para los problemas previsibles.

7. Evaluación de la relación costo/beneficio de cada alternativa.
No existe ninguna manera costeable para protegerse completamente contra todo tipo de riesgos, particularmente amenazas naturales; como consecuencia, siempre se tiene que tolerar algún riesgo residual.
Deberá determinarse la mejor solución desde el punto de vista costo/beneficio para cada proceso. Deben obtenerse los recursos para las pruebas, ya sean recursos físicos o mano de obra para realizarlas.

Si sabemos que una de las acciones a tomar requiere detener la operación, es necesario considerar una ventana de tiempo que permita su realización sin afectar el negocio de la empresa. Si el costo de la implantación de una acción, es demasiado alto y no representa ningún beneficio adicional a la organización, se puede reconsiderar y no tomar dicha acción.
La reiniciación del proceso normal no implica la cancelación del alternativo, salvo que deban utilizarse los mismos recursos. Si esto no es así, durante cierto tiempo, los procesos deberían ejecutarse en paralelo para asegurar que la reiniciación de la operación normal es correcta y, ante cualquier defecto, continuar con el de contingencia.

La tabla 4.10 nos ejemplifica las fases mencionadas hasta ahora.

Contingencia	Evaluación de Riesgos	Alternativas de solución	Costo	TRO
Desastres naturales	Actividades interrumpidas hasta solucionar problema	Uso de sistema alterno o adaptación de uno emergente.	Costo total Hardware e instalación.	Total: 5 dias. Parcial: 24 hrs.
Corte de energía eléctrica	Discontinuidad del trabajo	Avisar a mantenimiento y notificar a la compañía de luz.	Perdida del servicio	24 hrs.
Robo	Pérdidas parciales o totales, según la gravedad de los hechos	Activar la alarma, comunicar a encargado de seguridad y notificar a la policía.	Costo Hardware. Reposición de equipos. Perdida del servicio	Total: 72 hrs. Parcial: 12 hrs.
Virus informáticos	Pérdidas totales o parciales de la información almacenada.	Aislamiento, erradicación, instalación de hotfixes.	Evaluar daño ocasionado. Perdida del servicio	24 hrs.
Ataques internos	Pérdidas totales o parciales, vulnerabilidad del sistema.	Detección y contención.	Evaluar daño ocasionado. Perdida del servicio	24 hrs.
Problemas de comunicación del cliente con los servidores	Interrupción en las actividades hasta solucionar el problema.	Verificar configuraciones o buscar fallas en hardware.	Perdida del servicio	24 hrs.
Problemas en el cableado eléctrico.	Interrupción en las actividades hasta solucionar el problema.	Reparación o reposición del cableado.	Costo por metro de cable, Perdida del servicio	24 hrs.
Problemas con los recursos compartidos de la red	Interrupción en las actividades hasta solucionar el problema.	Verificar configuraciones o buscar fallas en hardware.	Perdida del servicio	24 hrs.
Caída de la base de datos	Interrupción en las actividades hasta solucionar el problema.	Detección del fallo y restauración de las operaciones	Perdida del servicio	24 hrs.
Caída temporal del servidor por falla mecánica	Evaluar costo de reparación del desperfecto mecánico.	Unificar trabajo con otro servidor (si hay otro)	Evaluar costo del daño. Perdida del servicio	24 hrs.
Pérdida total de un servidor	Evaluar costo de reparación o de reposición.	Unificar con otro servidor Restauración de copia backup	Costo del servidor. Perdida del servicio	48 hrs.
Falla total o parcial del cableado	Operaciones interrumpidas hasta solucionar el problema.	Reparación o reposición del cableado.	Costo por metro. Perdida del servicio	Parcial: 12 hrs. Total: 24 hrs.
Pérdida total o parcial de una estación de trabajo	Evaluar costos.	Reparación o reposición del equipo.	Costo de estación de trabajo. Perdida del servicio	Parcial: 12 hrs. Total: max. 48 hrs.

Tabla 4.10 Tipificación de contingencias

8. Documentación del plan de contingencia.
Crear un documento que mucha gente pueda tener como referencia es quizás lo más difícil del plan de contingencia. Una correcta documentación ayudará a la hora de realizar las pruebas. Debe contener:

- Objetivo del plan.
- Personas encargadas y sus respectivas responsabilidades.
- Modo de ejecución.
- Tiempo de duración.
- Costes estimados.
- Recursos necesarios.

Dado el hecho de que la tecnología de red evoluciona tan rápidamente, debería planificarse la actualización del plan de contingencia periódicamente, por ejemplo una vez al año. Aunque la redacción del plan inicial supondrá una gran cantidad de trabajo, una vez que se dispone del plan, las actualizaciones son relativamente fáciles. Será necesario realimentar el plan de acuerdo a los resultados obtenidos en las pruebas.

Hay que tener en cuenta que el plan de contingencia general o de continuidad de operaciones de la empresa contiene los planes de contingencia específicos para cada problema definido. Los distintos planes deben integrarse en un todo, considerando las posibles relaciones mutuas.

La documentación del plan de contingencia debe incluir:

- *Listas de notificación.-* Hay que cerciorarse de saber a quién notificar cuándo ocurre un desastre. Pueden existir otras personas u organizaciones identificadas con características o conocimientos especiales que puedan ayudar a minimizar el daño.
- *Prioridades y responsabilidades.-* Hay que centrarse en las prioridades establecidas. Las personas deben disponer de instrucciones y responsabilidades precisas.
- *Relaciones y procedimientos.-* Deberán documentarse las operaciones y la relación de tareas que muestren las labores de instalación y recuperación necesarias.
- *Información sobre adquisiciones y compras.-* Debe saberse cómo expedir una solicitud de compra y obtener los equipos. Es aconsejable disponer de copias de las facturas, recibos y demás para mostrarlos como prueba de compra. Tener a la mano una lista de 1os números de serie de los equipos hardware.
- *Diagramas de las instalaciones.-* Los diagramas de red simplifican en gran medida la labor de reconstruir la red. Brinda la posibilidad de emplear contratistas para realizar las instalaciones. Alguien experimentado, es capaz de realizarlo mejor y más eficientemente.
- *Asignación de etiquetas a los cables.-* No llevará mucho tiempo y evitará muchas confusiones con posterioridad.

- *Sistemas, configuraciones.-* Planifíquese instalar una configuración genérica que, como mínimo, permita ejecutar las aplicaciones de mayor prioridad sin problemas. Ya después será posible restaurar los PC con sus configuraciones anteriores.
- *Copias de seguridad.-* Asegurarse la disponibilidad de un sistema de copias de seguridad en funcionamiento. (por duplicado, archivar una dentro de la compañía y otra fuera de la misma) Si es posible, mantener un sistema de reserva.

Asegurar la disponibilidad de copias extra de la documentación para su depósito en cualquier otro lugar fuera del lugar de trabajo.

9. Verificación e implementación del plan

Una vez redactado el plan, hay que probarlo. Han de realizarse las pruebas no solo para verificar que el plan funciona, sin también para encontrar problemas y para poner en evidencia posibles carencias del plan.

Es necesario documentar las pruebas para su aprobación por parte de las áreas implicadas. La revisión debe ser periódicamente y por partes, acciones a realizar:

- Confirmar si las listas de notificación son actuales.
- De ser el caso, ir a conocer la instalación alterna.
- Realizar simulacros de contingencia: capacitar al personal en caída de sistemas o fallas de servidores.
- Verificar los procedimientos para almacenar y recuperar los datos.
- Comprobar el correcto funcionamiento del software encargado de realizar la recuperación de los datos
- Confirmar si pueden recuperarse aplicaciones de mayor prioridad.
- Una vez recuperada la información, verificar si el usuario puede acceder a ella. (Incluir información sobre el establecimiento de cuentas de usuario).

10. Validación, distribución y mantenimiento del plan de contingencia.

Es necesario que el plan sea validado por los responsables de las áreas involucradas. Cuando se disponga de un plan definitivo ya verificado, es necesario distribuirlo a las personas que necesitan tenerlo. Mantener una lista de todas las personas y ubicaciones que tienen una copia. Cuando se actualice el plan, sustituir todas las copias.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado.

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante futuras nuevas eventualidades.

4.4 SLA's (Service Level Agreement's)

La empresa proveedora del servicio de seguridad establece junto con el cliente las partes de su entorno computacional que requieren de monitoreo. Se optimizan los parámetros de configuración de los sistemas para proteger las aplicaciones y operaciones claves de la empresa y se implementan controles de seguridad para dar seguimiento a los cambios y amenazas a los sistemas. Se realiza un análisis que permite establecer la definición de niveles de servicio y penalizaciones que deberán comprometerse con el fin de cubrir las necesidades de respuesta y continuidad de la operación del cliente de acuerdo a sus necesidades operativas.

En las tablas 4.11 se ejemplifican los compromisos a los que debe estar obligado el proveedor externo de outsourcing.

Métrica	Compromiso	Comentarios
Disponibilidad de los dispositivos (firewall, IDS; control de accesos web y sistemas de detección de vulnerabilidades)	99.96%	La disponibilidad de los dispositivos de seguridad se considera sobre el tiempo que el dispositivo esté funcionando, no se considera el tiempo que tiempo que pueda estar el servicio fuera por causas de caída del enlace.
Tiempo de atención a fallas	Con base en la tabla de tipificación de fallas	Tiempo de atención a fallas en el ámbito de responsabilidad del SOC.
Tiempo de atención a requerimientos de cambios	Con base en la tabla de tipificación de cambio	Tiempo de atención a requerimiento de cambio en el ámbito de responsabilidad del SOC.
Tiempo de atención para la aplicación de parches y actualizaciones para los dispositivos.	Tiempo de atención 3 horas.	No se considera dentro de esta métrica la aplicacion de nuevas versiones de las aplicaciones ya que este tipo de cambios requieren una evaluación completa y una serie de pruebas.
Respuesta a ataques	Tiempo de atención 1 hora.	Tiempo de atención para la detección y contención con herramientas de seguridad
Entregables	Uno al mes dentro de los primeros 7 días.	Entrega de Reportes
Revisiones	Una vez al bimestre	Reuniones bimestrales para detección de necesidades. La fecha de la reunión se programará con 2 semanas de anticipación

Tabla 4.11 Niveles de Servicio (SLA).

Las tablas 4.12 y 4.13 muestran un estimado de los tiempos de atención que deben respetarse para cada falla o cambio.

Dispositivo	Actividad	Tipo de Requerimiento	Tiempo de Atención
Firewall **IDS** **Control acceso web** **Sistemas de detección de vulnerabilidades**	**Administración**	Cambio a la configuración de red	1 hr.
		Cambio a las reglas de configuración de seguridad	0,5 hr
		Baja temporal de un servicio	1 hr.
		Baja definitiva de un servicio	2 hr.
		Baja temporal de un equipo	2 hr.
		Baja definitiva de un equipo	2 hr.
		Alta de usuario	1 hr.
		Baja de usuario	1 hr.
		Cambio de privilegios de un usuario	2 hr.
		Cambio de password de un usuario	2 hr.
		Recuperación de una configuración o una bitácora	3 hr.
		Cambios de personal para solicitud de requerimientos	Programado
		Nueva Política	2 hr.
		Modificación de Políticas	2 hr.
		Baja de Políticas	2 hr.
		Movimiento físico del equipo	Programado
	Operación	Prueba de funcionalidad	Programado
		Ejecución de pruebas de vulnerabilidades	Programado
		Respaldo extraordinario	5 hr.
		Depuración de cuentas que no presenten uso en un período determinado	7 hr.
		Entrega mensual de reportes	Programado
	Mantenimiento de software	Actualización de Emergencia	3 hr.
		Actualización de Software	3 hr.
		Cambio de Versión	Programado
		Descontinuación - Cambio de Producto	Programado
		Actualización a la versión del Sistema Operativo	Programado

Tabla 4.12 SLA's de acuerdo al tipo de requerimiento de cambio

Herramienta	Actividad	Requerimiento	Tiempo de Atención
Firewall	Operación	Servicio de Internet no disponible	1 hr.
		http no disponible	1 hr.
		ftp no disponible	1 hr.
		Correo electrónico no disponible	1 hr.
		DNS no disponible	1 hr.
		Falla en conectividad con el Firewall	1,5 hr.
		Política mal configurada.	1 hr.
		No levanta el FW	0,5 hr
		No soporta el nivel de tráfico de la red.	1,5 hr.
		No reporta ningún evento a la consola.	1,5 hr.
		Equipo comprometido.	0,5 hr
		Falla en el Sistema Operativo	2.5 hr.
		Errores lógicos o físicos en el equipo.	1,5 hr.
		Log lleno	3 hr.
	Respuesta a ataques	Ataques en proceso, exitosos y recurrentes	0,5 hr
IDS	Operación	Falla en conectividad con el IDS	0,5 hr
		Política mal configurada.	1 hr.
		No levanta el IDS	0,5 hr
		No soporta el nivel de tráfico de la red.	1,5 hr.
		No reporta ningún evento a la consola.	1,5 hr.
		Equipo comprometido.	0,5 hr
		Falla en el Sistema Operativo	2.5 hr.
		Errores lógicos o físicos en el equipo.	1,5 hr.
		Log lleno	3 hr.
	Respuesta a ataques	Ataques en proceso, exitosos y recurrentes	0,5 hr
Control accesos web	Operación	Servicio de Internet no disponible	0,5 hr
		Política mal configurada.	1,5 hr.
		No levanta el Control de Accesos Web	0,5 hr
		No soporta el nivel de tráfico de la red.	1,5 hr.
		No reporta ningún evento a la consola.	1,5 hr.
		Equipo comprometido.	1 hr.
		Ataque en progreso	1 hr.
		Falla en el Sistema Operativo	2.5 hr.
		Errores lógicos o físicos en el equipo.	1,5 hr.
		Log lleno	3 hr.
	Fallas en control de acceso	Acceso no autorizado a sitios dentro de la base de datos	3 hr.
		Recurrencia en accesos no autorizados	3 hr.
Sistema de detección de vulnerabilidades	Operación	Política de scaneo mal configurada.	1,5 hr.
		No levanta el detector de vulnerabilidades	2.5 hr.
		Falla en el Sistema Operativo	2.5 hr.
		Errores lógicos o físicos en el equipo.	1,5 hr.
		Log lleno	3 hr.

Tabla 4.13 SLA's de acuerdo al tipo de falla

CONCLUSIONES

Cualquier sistema se encuentra expuesto ante amenazas causadas por vulnerabilidades conocidas que no han sido atendidas adecuadamente. Una infraestructura tecnológica de seguridad no garantiza que la información esté protegida si no se mantiene un constante monitoreo; los firewalls y los dispositivos para detectar y prevenir intrusos generan un gran número de alertas si no están actualizados; entonces nos encontramos ante una situación en la que no basta con solo monitorearlas, sino que se debe realizar un análisis sobre esta información para determinar su importancia y preparar una respuesta para prevenir o combatir el ataque, si es que lo hay.

Es necesario implementar esquemas que requieren de métodos especializados para supervisar las operaciones del sistema y el manejo de información de seguridad; por ello es indispensable contar con un procedimiento de respuesta a incidentes sobre los eventos y alertas que se registren dentro de la red mediante un sistema de correlación de eventos de seguridad que se encargue de analizar cada mensaje generado por las herramientas y darle el tratamiento adecuado.

Para definir un modelo operativo que cubra las necesidades de seguridad informática de una organización, se debe llevar a cabo la identificación y definición de necesidades operativas, servicios y aplicaciones críticas; arquitectura de seguridad, tamaño y crecimiento planeado. Deben definirse las políticas, lineamientos, reglamentos y estándares, de tal forma que garanticen el cumplimiento de los requerimientos establecidos; introducir controles de medición y monitoreo necesarios que validen el cumplimiento en la operación con el fin de determinar líneas de acción que minimicen las brechas que pudieran existir entre la operación o las necesidades de los servicios y la arquitectura definida.

Se requieren asesores expertos en seguridad que realicen auditorías programadas que garanticen la continuidad en el cumplimiento de las políticas de seguridad de la información establecidas por la empresa y así conocer el estado general de los sistemas: áreas que no cumplen y lineamientos para que esos sistemas se apeguen a las políticas; se deben optimizar los procesos y generar soluciones que se orientarán a minimizar los riesgos, además de un análisis de tendencias que ayude a determinar si su postura de seguridad está empeorando o mejorando, y cuáles son las razones. Además, es imprescindible que el área encargada de la seguridad y el área de recursos humanos trabajen juntos en la creación de campañas que promuevan las mejores prácticas en seguridad, creando así una cultura de la seguridad de la información.

Para cualquier empresa, sea del tamaño que sea, cumplir con todos estos requerimientos es una tarea muy difícil por lo que podemos decir que el outsourcing se ha vuelto una necesidad, más que una alternativa. Anteriormente, el outsourcing era considerado simplemente como un medio para reducir significativamente los costos; sin embargo en los últimos años ha

demostrado ser una herramienta útil para el crecimiento de las empresas; es por ello que las PyMEs en México encuentran en el outsourcing una excelente alternativa para satisfacer sus requerimientos de seguridad de la información.

Un servicio de seguridad informática proporcionado por outsourcing se enfoca a establecer el soporte de servicios como un conjunto de procesos integrados con la misión de lograr los objetivos, la continuidad y la calidad de los servicios de tecnologías de información; se deberá realizar un análisis de riesgos y junto con el cliente, en este caso, la PyME, determinar las prioridades de operación del negocio y establecer una política de seguridad organizacional clara que soporte las necesidades de toda la empresa. Se deberán identificar todas las vulnerabilidades, detallar las acciones correctivas y elaborar un plan, paso por paso, para implementar los procesos de seguridad contando con autonomía en la toma de decisiones para la aplicación de líneas de acción de seguridad pero siempre con apego a las necesidades de operación de la empresa; debe integrar sus procesos sin que se perciba que es independiente y mantener la operación con un control total de los procedimientos.

El outsourcing brindará vigilancia permanente de la infraestructura de seguridad informática para prevenir o dar solución a eventos de seguridad; debe garantizar la operación correcta y segura en las instalaciones de procesamiento de información; establecerá procedimientos para la administración y operación, así como controles para el acceso a la información con base en los requerimientos de seguridad del negocio que identifiquen y reduzcan riesgos, limiten el impacto y aseguren la reanudación de las operaciones esenciales dentro del tiempo requerido; se comprometerá a minimizar las interrupciones en las actividades del negocio y a proteger los procesos críticos por fallas o desastres mayores; deberá documentar todas las actividades de solución y prevención del evento, pues dicha información servirá como la base de conocimientos para la resolución de eventos similares en el futuro.

Por todo esto, el outsourcing está obligado a adaptarse a través de la experiencia, técnicas, conocimientos específicos y alta competitividad; requiriendo de capacitación y adecuación inmediata de su capital humano para servir de acuerdo a las expectativas, y brindar resultados de manera inmediata ya que deberá asignar y aceptar responsabilidades con un fuerte compromiso, convirtiéndose no solo en un proveedor externo sino un socio de negocio confiable que revise de manera regular el apego a la seguridad de los sistemas críticos de la empresa y mantenga un adecuado nivel de protección sobre los activos de la organización. Deben mantenerse márgenes operativos que eviten o minimicen la ocurrencia de disturbios y garanticen la continuidad y calidad de los servicios dentro de los valores indicados y no debemos olvidar firmar un contrato de confidencialidad ni establecer los niveles de servicio aceptables para la operación del negocio, así como las indicar las respectivas penalizaciones por incumplimiento de los acuerdos pactados.

Así pues, como hemos visto, el 99.8% de empresas en México son PyMEs y es difícil que puedan hacer grandes inversiones en tecnologías sofisticadas en la seguridad, contratar expertos o capacitar personal en seguridad. Incluso, aún teniendo el poder adquisitivo para sufragar todos los gastos que un buen esquema de seguridad requiere; la contratación de un proveedor especializado contribuye a la obtención de los objetivos organizacionales mediante la solución a través de un enfoque que combina infraestructura tecnológica y física, recursos humanos y la implementación de las mejores prácticas, mejorando así la postura de seguridad contando con la reacción oportuna ante un posible evento de seguridad informática y permitiendo a la PyME preocuparse exclusivamente por definir la funcionalidad de las diferentes áreas de su organización, lo cual les permitirá crecer y fortalecerse en sus respectivos nichos de mercado, contando con información oportuna, confiable y veraz; dejando que la empresa de outsourcing se ocupe de decisiones de tipo tecnológicos, manejo de proyecto, implantación, administración y operación de la infraestructura de seguridad.

Por ello las PyMEs, al igual que muchas de las grandes empresas internacionales, han encontrado en la contratación de un outsourcing a un proveedor especializado que ofrezca soluciones de seguridad integradas y una mayor efectividad de estos servicios obteniendo todos los beneficios de la TI, aumentado la productividad incrementando la calidad del servicio y apoyando la operación de la organización.

Para las PyMEs los resultados son ampliamente satisfactorios al contar con un outsourcing de seguridad informática. El poseer lo mejor de la tecnología sin capacitar personal de la organización para manejarla y contar con expertos para disponer de las soluciones que brindan los servicios de las tecnologías de información de forma rápida, para que sus negocios sean eficientes y competitivos favorece una acertada toma de decisiones con base en indicadores de TI. Por esta razón consideramos que el outsourcing es la mejor alternativa de solución de seguridad de la información para las empresas mexicanas.

Apéndice

Tecnologías de Firewall

1. Filtrado de Paquetes (Packet Filter)

Es el modelo más antiguo y sencillo, trabaja en los niveles de transporte y de red del modelo OSI y está conectado a ambos perímetros, interior y exterior, de la red. Ver Figura A.1.

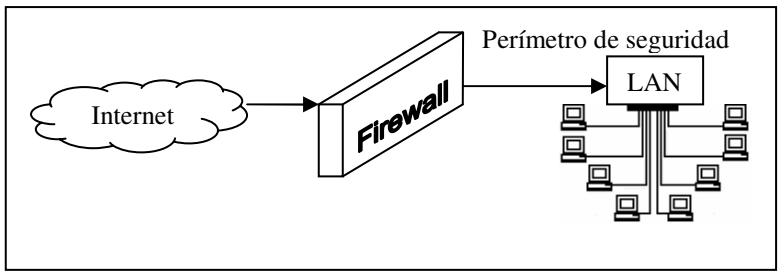


Figura A.1. Filtrado de Paquetes

Consiste en un dispositivo capaz de filtrar paquetes basado simplemente en aprovechar la capacidad de algunos routers para hacer un enrutado selectivo, es decir, para bloquear o permitir el tránsito de paquetes mediante listas de control de acceso (Access Control Lists, ACL) en función de ciertas características de las tramas.

Su funcionamiento es simple, se analiza la cabecera de cada paquete; se suelen contemplar campos como direcciones origen y destino, el protocolo utilizado, los puertos origen y destino, en el caso de TCP y UDP; el tipo de mensaje, en el caso de ICMP. Algunas implementaciones de filtrado permiten especificar reglas basadas en la interfaz del router por donde se ha de reenviar el paquete, y también en la interfaz por donde ha llegado hasta nosotros.

Esta tecnología es la más simple de implementar, en muchos casos sobre hardware ya ubicado en la red, y es la más utilizada en organizaciones que no precisan grandes niveles de seguridad. No obstante, elegir un firewall tan sencillo puede no ser recomendable en ciertas situaciones ya que no disponen de un sistema de monitoreo sofisticado, por lo que muchas veces el administrador no puede determinar si el router está siendo atacado o si su seguridad ha sido comprometida; además, las reglas de filtrado pueden llegar a ser complejas de establecer, y por tanto es difícil comprobar su corrección. Un listado de ventajas y desventajas de esta arquitectura puede observarse en la tabla A.1.

Es recomendable bloquear todos los servicios que no se utilicen desde el exterior, así como los paquetes con encaminamiento en origen activado (IP Forwarding).

Ventajas	▪ Económicos ▪ Tienen un alto nivel de desempeño ▪ Proporcionan una buena administración de tráfico ▪ Son transparentes para los usuarios conectados a la red. ▪ Permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en internet, puerto 80 abierto pero no acceder a la transferencia de archivos vía FTP, puerto 21 cerrado.
Desventajas	▪ No protege las capas superiores a nivel OSI. ▪ No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior. ▪ Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades. ▪ No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

Tabla A.1 Ventajas y desventajas del filtrado de paquetes

2. Puertas de enlace de aplicación (Proxy – Gateway de Aplicación)

Filtran tráfico a nivel de aplicación; para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones, programas para reenviar o bloquear conexiones a servicios. Estas aplicaciones son conocidas como servidores proxy y la máquina donde se ejecuta recibe el nombre de gateway de aplicación. Debe existir un proxy para cada protocolo y servicio que se desea filtrar: FTP, HTTP, SMTP, etc.

Cuando un usuario desea un servicio, lo hace a través del proxy. 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 devuelven a quien las solicitó. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma. Este tipo de firewalls no utilizan reglas de control de acceso pero en cambio aplican restricciones para garantizar la integridad de la conexión como filtrar comandos y estructuras incorrectas o no aprobadas de un protocolo o servicio específico. Su implementación puede observarse en la figura A.2.

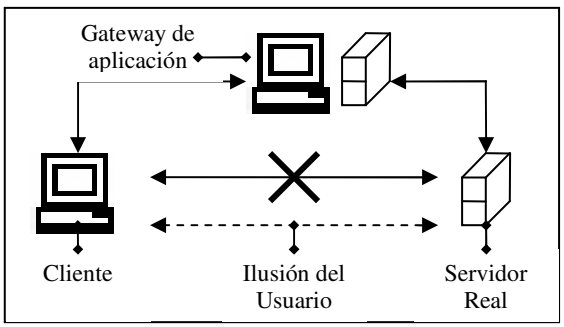


Figura A.2. Proxy server

Esta tecnología presenta ventajas y desventajas. Ver la tabla A.2.

Ventajas	▪ Permite únicamente la utilización de servicios para los que existe un proxy, por lo que si solo contiene proxies para telnet, HTTP y FTP, el resto de servicios no estarán disponibles a nadie. ▪ Es posible filtrar protocolos basándose en algo más que la cabecera de las tramas, lo que hace posible tener habilitado un servicio como FTP pero con órdenes restringidas; ▪ Permite un grado de ocultación de la estructura de la red protegida; el gateway es el único sistema cuyo nombre está disponible hacia el exterior ▪ Facilita la autenticación y la auditoría del tráfico sospechoso antes de que alcance el host destino y, ▪ Simplifica enormemente las reglas de filtrado implementadas en el router, que pueden convertirse en la fuente de muchos problemas de seguridad; sólo hemos de permitir el tráfico hacia el gateway, bloqueando el resto.
Desventajas	▪ No es transparente para el usuario final ▪ Cada servicio que deseemos ofrecer necesita su propio proxy. ▪ Se trata de un elemento más caro que un simple filtro de paquetes ▪ Su rendimiento es mucho menor, ya que puede llegar a limitar el ancho de banda efectivo de la red.

Tabla A.2 Ventajas y desventajas del gateway de aplicación

3. Puertas de enlace de nivel de circuito (Circuit Level Gateway)

Implementan el concepto de circuitos virtuales a través de redes que son separadas de manera lógica por el dispositivo. Los conceptos de NAT (Network Address Translation) y PAT (Port Address Translation) son aplicados por estos dispositivos para mantener una relación entre conexiones de las distintas redes a través de los circuitos virtuales. Para establecer una conexión entre ambas redes el cliente debe conectarse al dispositivo, quien a su vez se conecta con el servidor en la otra red; cliente y servidor nunca interactúan directamente y sólo ven al dispositivo como punto de entrada y salida hacia la otra subred.

Este tipo de firewall solo permite datos en su red que hayan sido solicitados por una computadora dentro de su red. Mantiene un registro de los pedidos de datos que salen y solo permite la entrada de datos que estén de acuerdo con estos pedidos. Una ventaja es que funciona como puente con la red que esta protegiendo, cualquiera que este buscando computadoras en la red solo podrá ver la dirección del firewall, pero no el resto de la red que esta siendo protegida, brindando una mayor seguridad para los usuarios internos de nuestra red, ocultando las verdaderas direcciones IP que formulan las solicitudes, y filtrando los paquetes que salen, pero sobre todo los que entran, para ser redirigidos hacia la máquina local que originalmente hizo la petición.

Los proxies trabajan a nivel de capa de sesión, presentación y aplicación en el modelo OSI. Esto es un avance sobre el filtrado de paquetes, ya que permite controlar las conexiones por puertos, pero la gran desventaja es que no verifica el contenido de aplicación de la comunicación.

4. Inspección de paquetes con estado (Stateful Packet Inspection, SPI)

Se caracteriza por controlar la comunicación desde la capa de red hasta la de aplicación, mantiene una tabla de estado de las conexiones TCP y maneja las comunicaciones UDP con una tabla apropiada para este. Este tipo de firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Combinan la velocidad y la flexibilidad de los filtros de paquetes con la seguridad de nivel de aplicación de los servidores proxy; han demostrados ser muy eficaces a la hora de hacer cumplir una directiva severa para el perímetro de red. Funciona examinando cada paquete cuando pasa a través de él y permite o deniega el paquete en función de si forma parte de un conjunto de reglas muy parecidas a las de filtrado de paquetes.

La desventaja es su costo, si bien este tipo de soluciones son muy recomendadas, generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas como en entornos bancarios ya que muchas organizaciones no pueden pagar este tipo de dispositivos.

En la figura A.3 podemos ver el flujo lógico que se lleva a cabo en una inspección de paquetes con estado.

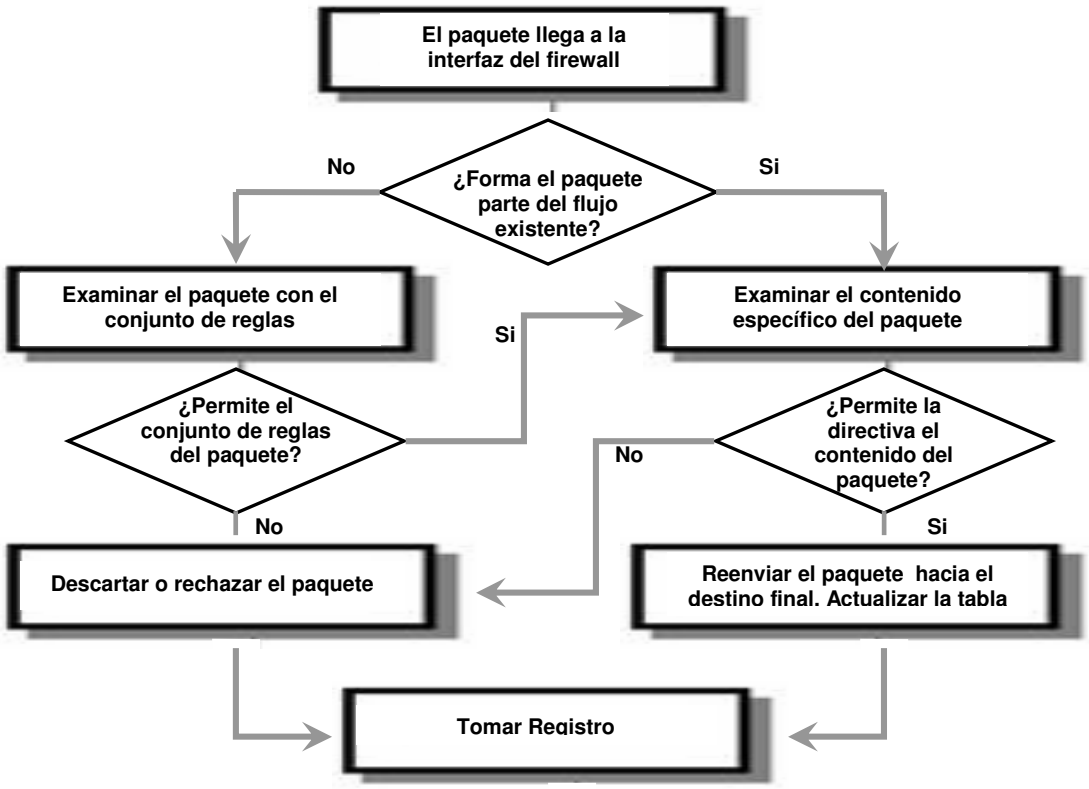


Figura A.3 Diagrama de flujo de SPI

Topologías de Firewall

Algunos diseños están compuestos por la unión de estas técnicas, como son:

1. Screened Subset

Intenta asilar el host bastión ya que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red.

Es un diseño seguro, pero también complejo; se utilizan dos routers, denominados exterior e interior, conectados ambos a la DMZ como se muestra en la figura A.4

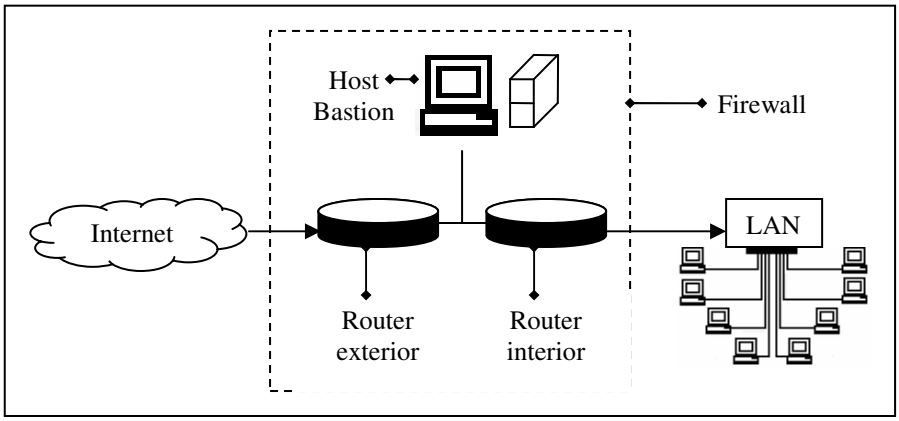


Figura A.4. Arquitectura Screened Subnet

En la DMZ se incluye el host bastión y también se podrían incluir sistemas que requieran un acceso controlado, como el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red. El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos, hacia la DMZ y hacia la red externa; mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la DMZ; incluso es posible implementar una zona desmilitarizada con un único router que posea tres o más interfaces de red, pero en este caso si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno; si un atacante accede al primer router puede aislar toda nuestra organización del exterior, creando una negación de servicio importante, sin embargo de menor gravedad que si lograra acceso a la red protegida, para lo cual deberá romper la seguridad del segundo router. Es posible definir mayores niveles de seguridad, agregando mas routers, es decir, varias DMZ en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas: así, el atacante habrá de saltar por todas y cada una de ellas para acceder a nuestros equipos; las reglas de filtrado aplicadas a cada router deben ser distintas ya que de no hacerse de este modo, niveles adicionales no proporcionan mayor seguridad pues se simplificarían a uno solo.

El principal problema relacionado con este diseño es que la mayor parte de la seguridad reside en los routers utilizados, las reglas de filtrado sobre estos elementos conllevan un cierto tiempo de procesamiento que en un momento dado podría afectar los tiempos de respuesta en la red, aunado a que pueden ser complicadas de configurar y comprobar, y dar lugar a errores que abran importantes brechas de seguridad en nuestro sistema. Sin embargo, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

- *Ocultamiento de la información*: los sistemas externos no deben conocer el nombre de los sistemas internos. El host bastión es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
- *Registro de actividades y autenticación robusta*: El host bastión requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
- *Reglas de filtrado menos complejas*: Las reglas del filtrado de los paquetes por parte del router serán menos compleja dado a que él sólo debe atender las solicitudes del host bastión.

Tiene la desventaja de no ser transparentes para el usuario ya que generalmente éste debe instalar algún tipo de aplicación especializada para lograr la comunicación. A esto se suma que generalmente son más lentos porque deben revisar todo el tráfico de la red.

2. Dual-Homed Host

Está formado por simples máquinas equipadas con dos o más tarjetas de red, en las que una de las tarjetas se suele conectar a la red interna a proteger y la otra a la red externa a la organización. En esta configuración el choke point y el host bastión coinciden en el mismo equipo. Ver Figura A.5

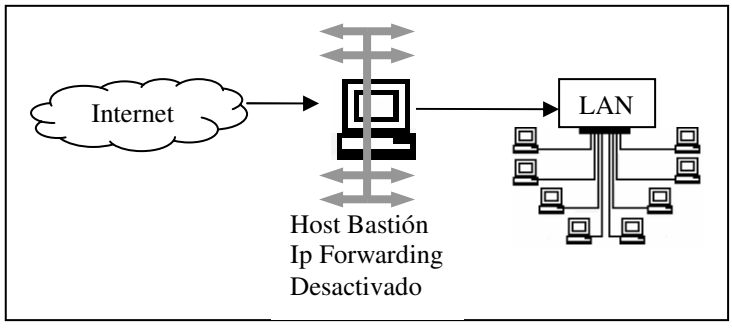


Figura A.5. Arquitectura Dual Homed Host

El sistema ha de ejecutar al menos un servidor proxy, concepto que explicaremos mas adelante, para cada uno de los servicios que deseemos pasar a través del firewall, se conectará al servicio exterior solicitado y hará de puente entre éste y el usuario interior. Es necesario que el IP Forwarding esté deshabilitado en el equipo: aunque una máquina con dos tarjetas puede actuar

como un router, para aislar el tráfico entre la red interna y la externa es necesario que el choke point no enrute paquetes entre ellas. Todo el intercambio de datos entre las redes se ha de realizar a través de servidores proxy, pero puede ser problemático el configurar cierto tipo de servicios o protocolos que no se diseñaron teniendo en cuenta la existencia de un proxy entre los dos extremos de una conexión.

3. Screened Host

El diseño screened host o choke-gate combina un router con un host bastión. El principal nivel de seguridad proviene del filtrado de paquetes, es decir, el router es la primera y más importante línea de defensa. En la máquina bastión, único sistema accesible desde el exterior, se ejecutan los proxies de las aplicaciones, mientras que el choke se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un reducido número de servicios. Ver figura A.6

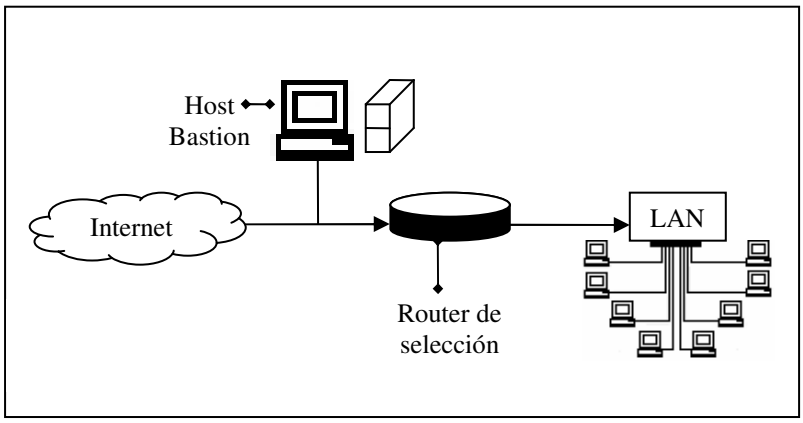


Figura A.6 Arquitectura Screened Host

Se sitúa el router entre la red exterior y el host bastión, así cuando una máquina de la red interna desea comunicarse con el exterior existen dos posibilidades:

- El choke permite la salida de algunos servicios a todas o a parte de las máquinas internas a través de un simple filtrado de paquetes.
- El choke prohíbe todo el tráfico entre máquinas de la red interna y el exterior, permitiendo sólo la salida de ciertos servicios que provienen de la máquina bastión y que han sido autorizados por la política de seguridad de la organización; obligando a los usuarios a que las conexiones con el exterior se realicen a través de los servidores proxy situados en el bastión.

La primera opción implica un mayor nivel de complejidad a la hora de configurar las listas de control de acceso del router, mientras que si elegimos la segunda, la dificultad está en configurar los servidores proxy, no todas las aplicaciones soportan bien estos mecanismos.

Desde el punto de vista de la seguridad es más recomendable la segunda opción, ya que la probabilidad de dejar escapar tráfico no deseado es menor. Por supuesto, en función de la política de seguridad que definamos, se pueden combinar ambas opciones, por ejemplo permitiendo el tráfico entre las máquinas internas y el exterior de ciertos protocolos difíciles de encaminar a través de un proxy o sencillamente que no entrañen mucho riesgo para nuestra seguridad y obligando para el resto de servicios a utilizar el host bastión.
Este diseño puede parecer a primera vista más peligroso que el basado en una simple máquina con varias interfaces de red; en primer lugar, tenemos no uno sino dos sistemas accesibles desde el exterior, por lo que ambos han de ser configurados con las máximas medidas de seguridad. Además, la mayor complejidad de diseño hace más fácil la presencia de errores que puedan desembocar en una violación de la política implantada, mientras que con un host con dos tarjetas nos aseguramos de que únicamente aquellos servicios con un proxy configurado podrán generar tráfico entre la red externa y la interna, a no ser que por error activemos el IP Forwarding. Sin embargo, aunque estos problemas son reales, se solventan tomando las precauciones necesarias a la hora de diseñar e implantar el firewall y definiendo una política de seguridad correcta. De cualquier forma, en la práctica esta arquitectura está cada vez más en desuso debido a que presenta dos puntos únicos de fallo, el choke y el bastión: si un atacante consigue controlar cualquiera de ellos, tiene acceso a toda la red protegida.

Se debe elegir qué elemento utilizar como bastión; mantener esta máquina especialmente asegurada es algo vital para que el firewall funcione correctamente, ya que va a soportar por sí sola todos los ataques que se efectúen contra nuestra red al ser elemento más accesible de ésta. Suele ser una buena opción elegir un servidor corriendo alguna versión de Unix, ya que aparte de la seguridad del sistema operativo tenemos la ventaja de que la mayor parte de aplicaciones de firewall han sido desarrolladas y comprobadas desde hace años. Como choke suele ser un router con capacidad para filtrar paquetes, aunque también puede utilizarse un sistema Unix para realizar esta función.

Los firewalls han agregado con el paso del tiempo muchas características como autenticación de usuarios, control de redes, antivirus, traducción de direcciones de red (NAT, network adress translation), VPN, alta disponibilidad y técnicas de administración mejoradas.

Traducción de direcciones de red (NAT, Net Address Translation)

TCP/IP se creó con un espacio de 2^{32} (4 billones) de direcciones, lo cual no es suficiente. Existen bloques de direcciones que nunca se utilizarán en Internet y son usadas para las redes privadas. Ver tabla A.3.

Dirección	Clase	Máscara	Rango
10.0.0.0	A	255.0.0.0	10.0.0.0-10.255.255.255
172.16.0.0	B	255.240.0.0	172.16.0.0-172.31.255.255
192.168.0.0	C	255.255.0.0	192.168.0.0-192.168.255.255

Tabla A.3 Direcciones privadas especificadas en el RFC 1918

Sin embargo, estas direcciones tienen que traducirse en direcciones públicas cuando atraviesan el firewall. Se cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único; de manera que las direcciones de host que se encuentran dentro de la red de confianza se denominan *locales* y las del lado externo del firewall son llamadas *globales*, por lo que es necesario considerar esto al implementar NAT en un firewall y por ello se hace separado de las directivas o conjunto de reglas.

NAT estático

Cuando los hosts tienen definidas sus direcciones locales y globales, y estas nunca varían. Realiza un mapeo en la que una misma dirección IP privada se traduce siempre una correspondiente dirección IP pública. Se utiliza cuando un dispositivo necesita ser accesible desde fuera de la red privada.

NAT dinámico

Cuando se hace corresponder un grupo de direcciones locales internas con un conjunto de direcciones globales. La NAT dinámica se implementa simplemente creando NAT estáticas cuando un host interno envía primero un paquete a través del firewall y NAT se mantiene en las tablas de firewall hasta que algún evento hace que finalice. La desventaja de la NAT dinámica es el límite de usuarios internos que pueden tener acceso a los recursos externos de manera simultánea. El firewall se quedará sin direcciones globales y no será capaz de asignar direcciones nuevas hasta que se comiencen a liberar. La ventaja de la NAT dinámica sobre la estática es en el ámbito de la seguridad, ya que aumenta la dificultad a los hackers de realizar correspondencias en la red protegida, ya que las direcciones son aleatorias y cambian constantemente.

Implementando esta forma de NAT se genera automáticamente un firewall entre la red pública y la privada, ya que sólo se permite la conexión que se origina desde ésta última.

Traducción de direcciones de puerto (PAT, Port Address Translation)

Con la PAT todo el espacio interno para direcciones locales se puede hacer corresponder con una única dirección global. Esto se hace modificando las direcciones de puerto y manteniendo una tabla de conexiones abiertas. Esto beneficia la conservación de direcciones porque las conexiones salientes de toda la organización se pueden hacer corresponder con una única dirección IP. PAT proporciona un mayor nivel de seguridad porque no se puede utilizar para conexiones entrantes. Una desventaja de PAT es su limitación para realizar conexiones por un par de puertos específicos como con los protocolos orientados a la conexión como TCP, ya que al llegar al firewall éste le asignará un puerto aleatorio nuevo.

Estas traducciones de dirección se almacenan en una tabla, para recordar que dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. De esta forma, muchos host que se encuentran detrás del firewall pueden turnarse o compartir direcciones públicas cuando se tenga acceso a Internet.

Es la implementación más utilizada ya que toma múltiples direcciones IP privadas y las traduce a una única dirección IP pública utilizando diferentes puertos. Esto se conoce también como Hide NAT

Sistemas de Prevención de Intrusos (IPS, Intrution Detection System)

La tecnología IDS había estado bajo la sombra de una administración compleja que fundamentalmente era reactiva, por esta razón la industria de seguridad informática resolvió volcarse hacia el desarrollo de IPS atendiendo las debilidades de los IDS, cuyo mecanismo de defensa era el uso de tecnologías como detección por firmas o patrones (Signature based) y detección de situaciones anómalas (Anomaly based);

La tecnología IPS permite a las organizaciones, proteger los activos críticos en una forma efectiva y proactiva, más que sólo emitir alertas en una consola luego de que los ataques han sucedido. Los IDS descubren un intento de ataque o intrusión y los IPS bloquean el ataque antes de que este llegue a su objetivo. Es un dispositivo de seguridad que provee de un control de accesos.

Los IPS a diferencia de los firewalls toman decisiones en base al contenido del paquete de red a nivel aplicativo, puesto que los firewalls lo toman en base a una dirección IP origen otra de destino, el protocolo y puerto.

Igual que dentro de los IDS, los IPS existen de host (HIPS) o a nivel red (NIPS). Ahora bien, dentro de los NIPS existen:

- *Content Based*.- Inspeccionan el contenido de los paquetes de red en patrones (firmas). Detectan y previenen exitosamente una gran cantidad de ataques ya conocidos, así como la actividad de códigos maliciosos.
- *Protocol Analisys*.- La clave para el desarrollo de los IDS/IPS fue el uso de analizadores de protocolo. Estos pueden decodificar los protocolos de la capa de aplicación, como lo son el HTTP o FTP. Con esto los IPS son capaces de detectar cualquier comportamiento anómalo dentro de los protocolos.
- *Rated Based*.- Son principalmente desarrollados para prevenir ataques de negación de servicio (DoS). Al principio trabajan monitoreando y aprendiendo comportamientos normales de la red, después se colocan en modo protección y empiezan a comparar el tráfico en tiempo real con las estadísticas almacenadas. Una vez que un ataque es detectado mediante un comportamiento extraño en la red, el IPS empieza a tomar medidas bloqueando el tráfico anómalo y colocando las direcciones IP's que atacan en una especie de lista negra.

La principal defensa que nos brindan estos dispositivos son ataques de DoS, código malicioso, exploits, backdoors y spyware; y es usado también para bloquear actividades que no cumplan con las políticas de seguridad de una empresa como es el tráfico de Peer-to-Peer y el de mensajería instantánea.

Arquitectura Interna de un IPS

Los IPS tienen dos sub-unidades. La primer parte son búsqueda de patrones, la cual es hecha por la unidad rápida, responsable por pasar el trafico normal lo mas rápido posible pero no siempre es suficiente para capturar todas las intrusiones, las cuales pueden producir falsos-positivos. La segunda parte esta formada por una lógica más compleja, responsable por hacer lo mejor posible para detectar la intrusión analizando el trágico usando expresiones regulares. Esto es realizado por la unidad lenta. Cuando un simple patrón es encontrado por la unidad rápida, esta se tiene que volver a analizar por la unidad compleja/lenta, para lograr un mejor resultado.

El principal problema con los IPS's es lograr una buena relación entre velocidad y calidad. La mayor parte del tráfico necesita pasar por la parte lenta pues es necesario para un mejor análisis para saber si es un ataque o no.

Los IPS conforman las nuevas tecnologías proactivas de seguridad informática para proteger servidores y redes que cuentan con diversa herramientas para bloquear efectivamente ataques de hackers externos y/o internos, de amenazas tanto conocidas como desconocidas.

Bibliografía

Libros

HACKERS EN LINUX. Secretos y soluciones para la seguridad de Linux. Brian Hatch, James Lee, George Kurtz, Editorial McGraw-Hill, Segunda edición, pags. 4-5, 144-155, 509-540

The Information Security Dictionary, Gattiker Urs, Editorial Kluwer Academic Publishers, Primera Edición 2004, pags. 87-90, 244-245, 272-278, 315-316.

Inside Network Perimeter Security, Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, Editorial Sams Publishing, Segunda Edición 2005, pags. 177-206, 286-206, 312- 461, 481-597

Defining Incident Management Processes for CSIRTs: A Work in Progress, Chris Alberts, Editorial Camegie Mellon University, Primera Edición 2004, pags 15-20, 94

The Best Damn Firewall Book Period, Dr. Thomas W. Shinder, Cherie Amon, Robert J. Shimonski, Editorial Syngress Publishing, Inc., Primera Edición 2003, pags. 54-118, 577-582, 1239-1260

The CISSP Prep Guide, Ronald L. Krutz and Russell Dean Vines, Editorial Wiley Publishing Inc. Segunda Edicion 2004, pags. 4-15, 18-23, 24, 56-57, 133-136, 166-176, 184-187

Mesografìa

Seguridad de la Informacion, Donald R. Glass, Universidad CAECE de Argentina.
http://www.caece.edu.ar/Cursos/images/infosec109-216.pdf

SNORT - Lightweight Intrusion Detection for Networks, Martin Roesch
http://www.snort.org/docs/lisapaper.txt,

How to Guide-Implementing a Network Based Intrusión Detection System, Brian Laing and Jimmy Alderson, Internet Security Systems año 2000
http://www.snort.org/docs/iss-placement.pdf

Definiendo las Nuevas Fronteras en Seguridad y Continuidad de Negocio, Alejandro Florean Rodríguez, IT Security and Business Conference México 2005
http://www.idc-eventos.com/security05/agenda.html

Gobernabilidad de las TI, Una Moda o una Necesidad; Alejandro Florean Rodríguez, Corporate Connection Forum 2005
http://www.sterlingcommerce.com.mx/PDF/GobiernoCorporativo/Gobernabilidad%20de%20las%20TI%2028062005.pdf

The Computer Crime and Security Survey, hecho por CSI con la participacion del San Francisco Federal Bureau of Investigation (FBI)
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Seguridad en UNIX, Antonio Villalón Huerta, GNU Free Documentation License, 2002
http://www.rediris.es/cert/doc/unixsec/unixsec.pdf

Diario Oficial de la Federación del día 30 de diciembre de 2002

Censo Económico 2004
http://www.inegi.gob.mx/est/contenidos/espanol/proyectos/censos/ce2004/pdfs/resultados_grals.pdf

http://www.siem.gob.mx/portalsiem/

http://www.cybsec.com

http://www.gocsi.com/awareness/publications.jhtml

http://www.contactopyme.gob.mx

http://www.tuobra.unam.mx/publicadas/040702105342.html