INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

Curso *online*: **Seguridad en Redes WAN e Internet**

Módulo1 CONCEPTOS GENERALES DE SEGURIDAD INFORMÁTICA

Autores: Daniel Díaz y Andrés Marín

Índice de contenidos

INTRODUCCIÓN

Esta lección trata de encuadrar la seguridad de las redes de ordenadores dentro del contexto general de seguridad de los sistemas de información.

Se pretende mentalizar en la idea de que la seguridad en redes no se debe plantear como una actuación aislada y puntual. Cualquier actuación en seguridad debe responder a un planteamiento global acorde con una estrategia y definida en la Política de seguridad de la Organización.

También se efectúa una aproximación general de los aspectos a contemplar en la seguridad en redes y en Internet en particular, con la finalidad de dar coherencia al contenido del resto de las lecciones, sin obligar a seguir un orden estricto de exposición.

OBJETIVOS

Los objetivos de esta lección son:

- Formalizar el término seguridad de los sistemas de información.
- Conocer los tipos de medidas de protección a implantar: organizativas, técnicas y físicas, y la normativa legal a la que se deben adaptar y cumplir
- Conocer los aspectos y actuaciones que debe contemplar un Plan de Seguridad de los Sistemas de Información.
- Analizar los principios y consideraciones a tener en cuenta en la definición de las Políticas de Seguridad de los Sistemas de Información de las organizaciones.
- Conocer las características generales de la seguridad en redes: concepto de red, amenazas y elementos de protección a implantar para asegurar las conexiones con otras redes y en particular con Internet.

CAPÍTULO 1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

En las sociedades avanzadas del siglo XXI, la información es un bien más del activo de las empresas u organizaciones y, en muchos casos, prevalente sobre los restantes. En cualquier organización, la dependencia de sus sistemas de información (SI) es tal que, si dejan de funcionar puede acarrear la paralización de la empresa. Es obvio que se requieren garantías de que la información y las tecnologías que la tratan sean fiables y confiables.

A lo largo de estos apuntes siempre que, genéricamente, se utilice el término Seguridad, implícitamente, nos referiremos a la Seguridad de los Sistemas de Información.

El objetivo de la Seguridad es evitar los riesgos potenciales, tanto accidentales como intencionados, de ataque, robo o daño que puedan ocasionar la interrupción total o parcial de las actividades del negocio.

La implantación de la microinformática, los sistemas abiertos, el uso común de redes y la explosión de Internet hacen que el acceso a la información ya no esté limitado a unos pocos, lo cual implica, al mismo tiempo, que los Sistemas de Información (SI) estén expuestos a múltiples amenazas, "democratización del uso y del delito".

Vaya por delante que la Seguridad es un campo pluridisciplinar y que avales, incluso mínimos, de su correcto funcionamiento sólo se pueden obtener de la conjunción de sólidas medidas técnicas, sensatamente gestionadas y adecuadamente reguladas, lo que constituye una de las causas de la dificultad que entraña esta materia.

CAPÍTULO 2 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

En una primera aproximación puede establecerse que seguridad significa protección de bienes (llamados también activos o recursos).

Una definición más estricta puede expresarse como: “Calidad relativa, resultado del equilibrio entre el riesgo y las medidas adoptadas para paliarlo”, así, a mayor riesgo mayores deberán de ser las medidas de protección, lo que se conoce como principio de proporcionalidad**.** En esta acepción el riesgo de un activo es una combinación de las amenazas a las que está expuesto, sus vulnerabilidades y el valor del mismo, por consiguiente el riesgo será nulo cuando alguno de estos tres elementos sea nulo. Ya que las amenazas no se pueden evitar y normalmente todos los bienes siempre tienen un valor, la única vía para disminuir el riesgo es disminuir las vulnerabilidades mediante la adopción de las pertinentes medidas de seguridad.

La seguridad de la información comprende tanto la seguridad en el ordenador como en las comunicaciones. El objetivo de la seguridad en el ordenador es preservar los recursos de cómputo contra usos y abusos no autorizados, así como proteger los datos de daños, revelaciones y modificaciones accidentales o deliberadas. La seguridad en las comunicaciones tiene como objetivo proteger los datos durante su envío por las correspondientes redes.

La norma ISO 7498-2 define un servicio de seguridad como la prestación de un sistema basado en tecnologías de la información que contribuye a incrementar la seguridad del mismo.

Sin embargo, mejor que una definición formal de seguridad de la información, los expertos prefieren, por ser más útil, postular los objetivos de la misma, y los expertos coinciden en establecer como objetivos de la seguridad de la información la protección de la confidencialidad, integridad y disponibilidad de la misma:

- Confidencialidad, que la información sea revelada exclusivamente a los usuarios autorizados (personas, entidades, programas, etc) en la forma y tiempo determinados. En el secreto debe incluirse, no sólo el de los datos, sino también el del flujo de información.
- Integridad, que la información sea modificada (incluyendo su creación y borrado) sólo por el que esté autorizado. La integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta
- Disponibilidad, que la información sea utilizable cuándo y cómo lo requieran los usuarios autorizados.

Para estas tres características no existe una priorización universalmente aceptada, cada una será más o menos importante según la naturaleza de la información y de la empresa u organismo que se trate. Por ejemplo, la confidencialidad puede ser de primordial importancia en el departamento de diseño industrial de una empresa (para prevenir el espionaje industrial); mientras que la integridad puede ser la característica clave en un sistema de transferencia de fondos; por último, la disponibilidad quizá sea la característica mas apreciada en un sistema de producción industrial o en un sistema para un censo electoral. Además de estos objetivos, algunos sistemas requieren del no repudio, es decir, que una vez realizada una transacción ambas partes tengas pruebas que atestigüen que la otra parte ha aceptado la transacción:

- el que inicia la transacción que dispondría de una prueba de no repudio del destino, y
- el que completa la transacción que dispondría de una prueba de no repudio del origen.

CAPÍTULO 3 MEDIDAS DE PROTECCIÓN

Desde el punto de vista general la seguridad se centra en dos aspectos, uno técnico, consistente en una larga lista de herramientas tanto software como hardware, y el otro considera el factor humano, es decir el conjunto de personas encargadas de definir la política de seguridad, implantar el sistema de seguridad, administradores y todas aquellas personas que utilizan dicho sistema.

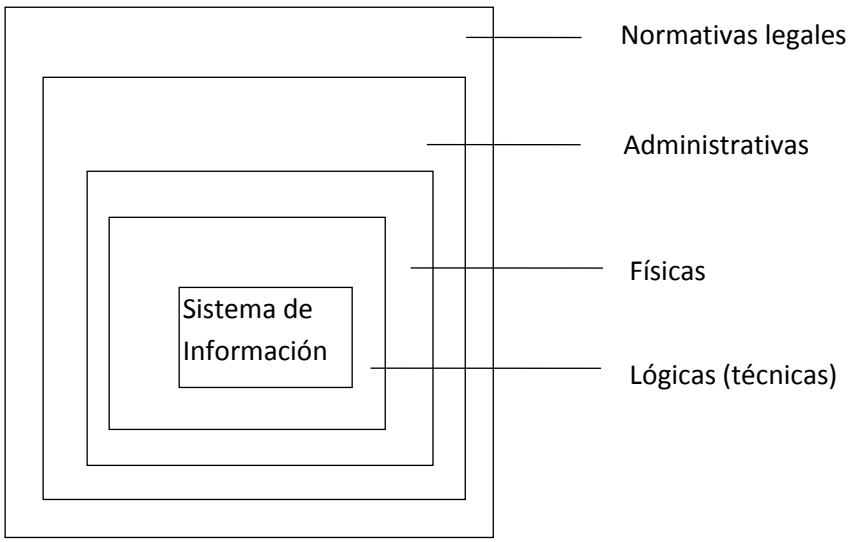
La seguridad es un concepto relativo, inalcanzable en plenitud, y que por cuantiosas que sean las inversiones en ella, siempre queda un riesgo residual que es imposible eliminar. La seguridad al 100% no se logra nunca, los controles (medidas) deben ser proporcionales a los riesgos, la falta de protección de los recursos informáticos es muy peligrosa pero el exceso es muy costoso. Es necesario identificar en donde podría suceder algo, que impacto tendría y cuanto costaría eliminar el riesgo o disminuir la probabilidad de ocurrencia, es muy importante sopesar los beneficios que nos reportan las medidas de seguridad con respecto a los recursos que queremos dedicar.

Conforme los Sistemas de Información se han hecho más complejos, se han puesto de manifiesto un mayor número de puntos vulnerables y una mayor facilidad para perpetrar ataques contra ellos. Existen dos razones fundamentales para que esto suceda:

El número de posibles atacantes y su imaginación crece rápidamente ante las posibilidades de obtención de beneficios.

Los medios disponibles para poder vulnerar un sistema son tan sofisticados como el sistema mismo puesto que tienen el mismo origen tecnológico.

Aunque la seguridad se apoya en la integración de un conjunto de medidas entrelazadas entre sí, para facilitar su análisis y comprensión, las medidas de protección se han venido clasificando en tres grandes tipos: lógicas, físicas y administrativas, todas ellas bajo el amparo de las normativas legales, que se pueden representar mediante el siguiente esquema de capas:



3.1. MEDIDAS DE PROTECCIÓN TÉCNICA (O LÓGICAS)

Las medidas técnicas pretenden proteger tanto el software como los datos, y pueden implementarse en dispositivos hardware o en productos software.

Los aspectos más notables de estas medidas de protección se centran en las siguientes técnicas o elementos:

a. ***Criptografía*** Cualquier estudio, por superficial que sea, de los aspectos técnicos de la seguridad debe comenzar por la criptografía, la criptografía es la base de la mayoría de los servicios de seguridad: confidencialidad, integridad, autenticación y no repudio.

Con la sociedad de la información la criptografía ha experimentado un fuerte desarrollo, que ha originado la aparición continua de nuevos y complejos algoritmos criptográficos.

b. ***Sistemas operativos*** Un sistema operativo seguro tiene que garantizar la disponibilidad de los recursos y la integridad de los datos, para lo cual, como mínimo, debe instrumentar los siguientes servicios o funcionalidades:
   - identificar y autentificar a todos los usuarios
   - controlar el acceso a los recursos y activos de información
   - contabilizar todas las acciones realizadas por los usuarios (o procesos invocados por ellos)
   - auditar los acontecimientos que puedan representar amenazas a la seguridad

c. ***Bases de datos*** Aunque los Sistemas Operativos se encarguen de algunos aspectos generales y primarios de la seguridad de las BD, los Sistemas Gestores de Base de Datos (SGBD) deben garantizar la seguridad de las propias Bases de Datos desde los aspectos formales a los relacionados con la semántica de los datos contenidos en las mismas.

d. ***Seguridad en redes*** Dentro de las medidas técnicas o lógicas se suele incluir la seguridad en redes. En el presente, las redes de ordenadores son las TIC más expuestas, lo que constituye un motivo de especial preocupación para las organizaciones, que no pueden prescindir, sin exponerse a ser marginadas por el mercado, de interconectar sus equipos aun a pesar de los riesgos que ello comporta.

Un elemento de riesgo muy presente en los sistemas de hoy en día lo constituye las tendencias de ***cloud computing*** y ***bring your own device*** *(BYOD)*. Ambas tendencias son imparables en las organizaciones de hoy en día y enfrentan a los departamentos de sistemas y en concreto a los responsables de seguridad ante los nuevos riesgos que comportan alojar datos sensibles en la nube (google drive, Dropbox, etc.) y ante el desafío que los usuarios utilicen sus dispositivos personales, a menudo no gestionados por los responsables de sistemas de la organización para actividades relacionadas con la actividad de la organización.

3.2. MEDIDAS DE PROTECCIÓN FÍSICA

El término seguridad física se usa para describir las medidas que tratan de proteger al ordenador y a su entorno de amenazas físicas externas a los mismos.

Las medidas de protección físicas son, probablemente, las primeras que se adoptan en todas las instalaciones informáticas. Ello es debido a dos factores: por un lado, aunque la probabilidad de que se produzca un incendio o una inundación es mucho menor que la

probabilidad de ocurrencia de otras amenazas, ante una catástrofe de este tipo las perdidas serían completas. Por otra parte, estas medias de protección son fáciles de tomar, su costo no es excesivo y su mantenimiento no ofrece dificultades especiales.

3.3. MEDIDAS DE PROTECCIÓN ADMINISTRATIVAS Y ORGANIZATIVAS

Se ocupan de dictar controles de índole administrativa y organizativa para instrumentar, reforzar o complementar las restantes medidas; es decir tienen que ver con:

- El establecimiento de una política de seguridad
- El análisis de riesgos y los planes de contingencia
- La asignación de responsabilidades
- La política de personal

3.4. NORMATIVA LEGAL

Comprenden el conjunto de disposiciones legales adoptadas por los poderes competentes para regular y proteger, vía sanciones penales o administrativas, la información y los sistemas y equipos que la tratan.

En España, se han promulgado bastantes leyes específicas para proteger la información, entre ellas podríamos citar:

- La Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (protección vía penal de datos sensibles e introducción, del fraude informático)
- La Ley Orgánica 15/1999, de 13 de Diciembre, (B.O.E. de 14 diciembre de 1999) de Protección de Datos de Carácter Personal (LOPD) (protección, vía administrativa, de datos personales)
- El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.
- La Ley de Propiedad intelectual (protección de los derechos de autor y editor del software)
- La Ley de Facturación Telemática (que obliga a implantar mecanismos de seguridad que aseguren la integridad y exactitud de la información transmitida por medios telemáticos)
- La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones
- La Ley 59/2003, de 19 de diciembre, de firma electrónica
- El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General de Estado.
- Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública, sobre los “Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades”

- **Ley 9/2014**, de 9 de mayo, General de Telecomunicaciones, en su Disposición final segunda, modifica la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Esta reforma recoge algunos cambios que son esenciales para la seguridad en el ciberespacio porque es la primera vez que esta ley utiliza el término Ciberseguridad y reconoce el papel fundamental que los Equipos de Respuesta de Incidentes de Seguridad (CERT) desempeñan a la hora de reducir el impacto de los ciberataques y ciberamenazas.

CAPÍTULO 4 PLANES DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Una solución de seguridad completa requiere algo más que la última tecnología. Son componentes críticos la existencia de una estrategia de seguridad, la gestión del riesgo, una política de seguridad actualizada, una organización que asuma la responsabilidad de la seguridad, un plan de divulgación y unas normas consistentes para la implantación de la tecnología.

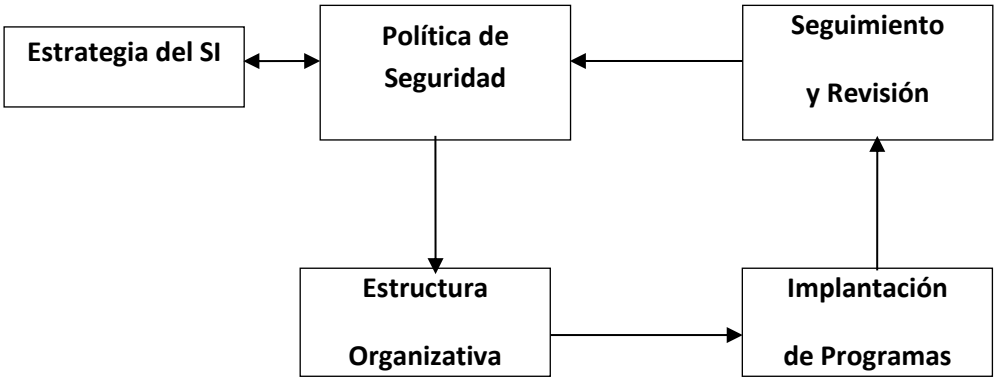
La Dirección de la Empresa u Organización debe establecer las directrices de la política de seguridad y adoptar el firme compromiso de su cumplimiento. Este compromiso debe estar inmerso en la estrategia de la organización, plasmado en una política de seguridad y desarrollado en los correspondientes programas de seguridad.

La Estrategia de Seguridad pretende introducir a la Dirección de la organización en la importancia de la seguridad de la información y su imprescindible compromiso con ella.

En esencia, se trata de fomentar un foro de discusión para generar una visión básica de la seguridad a fin de:

- Definir y formalizar el papel de la Dirección en la seguridad, y conseguir un adecuado nivel de conocimiento, concienciación y compromiso interno.
- Definir el modelo organizativo con el que se gestionará la seguridad (responsables de seguridad, comités de seguimiento…)
- Servir de base para el desarrollo de las actividades subsiguientes de generación de políticas y procedimientos operativos, así como todas aquellas acciones de implantación que deban llevarse a cabo.

La Seguridad no debe considerarse como un concepto aislado, debe influir en la política y estructura técnica subyacente a la estrategia de los SI.
La seguridad debe ser dinámica y estar en constante revisión y actualización. Conceptualmente es un proceso cíclico que se puede representar de la forma:



La implantación de productos y tecnologías para garantizar la seguridad de sistemas de información, puede resultar superflua o incluso contraproducente cuando no se plantea dentro de una concepción global de la seguridad.

CAPÍTULO 5 POLÍTICAS DE SEGURIDAD

Una política de seguridad es una declaración de intenciones de alto nivel que proporciona las bases para definir y delimitar responsabilidades en las actuaciones técnicas y organizativas que se requieran en relación con la seguridad de los SI (SSI). La política de seguridad de los SI debe ser formalmente acordada y documentada.

Una política de seguridad es un conjunto de principios y reglas, donde se especifica como se gestionará la protección de los activos de información de una manera consistente y efectiva

Definir una Política de Seguridad consiste en especificar los requisitos de protección de la información, los controles necesarios para protegerla y fijar las responsabilidades relativas a su protección.

Una Política de Seguridad debe:

- Alinear los requisitos de seguridad de la información con las necesidades de negocio de la empresa u organización.
- Fomentar el apoyo de la Dirección a la seguridad.
- Planificar y presupuestar la seguridad para hacerla posible y fácil de implantar.
- Establecer las responsabilidades en la gestión de la seguridad.
- Promocionar la divulgación, educación y formación en seguridad.
- Dejar patente a los usuarios la necesidad de la seguridad de la información y cómo ellos pueden contribuir a alcanzar los objetivos de seguridad.
- Facilitar la implantación de los procedimientos y mecanismos de seguridad.

La política de seguridad debe describir qué se intenta proteger y por qué; no debe describir detalles del cómo. Es mucho más útil tener un documento que describe “qué” y “por qué” en términos que todas las personas de la organización puedan entender, que un documento que describa “cómo” pero que nadie, excepto el equipo técnico, puede entender.

Una política de seguridad debe establecer expectativas y responsabilidades para todos los participantes del sistema, para permitirles saber qué esperar los unos de los otros. La política también debe especificar quienes tendrán la autoridad para tomar las correspondientes medidas correctivas y dar indicaciones sobre la clase de sanciones que se pueden imponer.

La propia política de seguridad debe prever su revisión, se debe evitar que una vez establecida se olviden de ella para siempre. Las necesidades de una organización cambian con el tiempo, y las políticas antes adecuadas pueden volverse demasiado estrictas o demasiado laxas.

5.1. PRINCIPIOS GENERALES DE SEGURIDAD

Han sido numerosos los intentos de establecer unos principios generales que pudieran considerarse como la Carta Magna de la seguridad de los sistemas de información; entre los intentos más notables están los auspiciados por la OCDE (Organización de Cooperación y Desarrollo Económico), y por la ISSA (*Information Systems Security Association*).

La OCDE, en una recomendación de 1992, propuso, los principios fundamentales siguientes:

- Principio de contabilidad (la responsabilidad del uso de los recursos debe ser explícita y exigible)
- Principio de concienciación (todas las partes implicadas deben ser sensibilizadas sobre las amenazas a la información y las medidas de seguridad de la misma)
- Principio de ética (la información y los sistemas de información deben ser usados con arreglo a los Códigos de Conducta Ética de los profesionales de la seguridad)
- Principio de multidisciplinariedad (las medidas de seguridad deben ser multidisciplinares: técnicas, administrativas, organizativas, etc.)
- Principio de Proporcionalidad (los niveles de seguridad y sus costes deben ser apropiados y proporcionales a los riesgos de la información)
- Principio de integración (las medidas, prácticas y procedimientos deben estar coordinados e integrados entre sí, para constituir un todo coherente y homogéneo)
- Principio de acompasamiento (las instituciones públicas y privadas, nacionales e internacionales deben actuar coordinadamente)
- Principio de reevaluación (la seguridad debe evaluarse periódicamente)
- Principio de democracia (la seguridad debe ser sopesada con los derechos de los usuarios y de todos los individuos involucrados)

ISSA, propuso, también en 1992, además de los principios generales establecidos por la OCDE, los siguientes:

- Principio del mínimo privilegio. Propugna que cualquier sujeto (usuario, administrador, programa, sistema o lo que sea) debe tener sólo, y no más, los privilegios que necesita para cumplir con las tareas que tenga asignadas.
- Principio de separación de tareas y responsabilidades. Establece que las responsabilidades se deben separar para que los que tienen que vigilar el cumplimiento de una norma no puedan utilizar los recursos sujetos a esa norma.
- Principio de continuidad. Para que sean efectivas, las medidas de seguridad deben establecerse para ser aplicadas de forma continua.
- Principio de anticipación. La mayoría de las medidas de seguridad se basan en la

prevención de riesgos, disminuyendo las vulnerabilidades de los activos. Siempre hay que tener presente la cuestión "Que pasaría si se produjese tal o cual incidente".

CAPÍTULO 6 INTRODUCCIÓN A LA SEGURIDAD EN REDES

Una red de ordenadores se puede definir como un entorno de cómputo con más de un procesador independiente.
Las redes de ordenadores han modificado el panorama de la informática, las redes se han convertido en una parte tan indispensable de la vida de muchas personas, que ahora es difícil imaginar utilizar la informática sin ellas.
La implantación de redes conlleva la aparición de nuevos problemas de seguridad derivados de que:

- Existen muchos más puntos de ataque y más posibilidades de llevarlos a cabo.
- Compartir recursos implica que cada usuario accede a la red a través de nodos diferentes, con controles de acceso distintos y con la posibilidad de que el control de acceso realizado por un sistema no sea suficientemente bueno para otro.

La realidad de las organizaciones y empresas ha cambiado radicalmente, apareciendo nuevos retos de seguridad a los que es necesario enfrentarse. Estos retos provienen de:

a) La existencia de nuevos usuarios internos y externos:
Todos ellos necesitan acceder a información crítica de la compañía y lo hacen a través de redes públicas como Internet.
b) La necesidad de interconexión de áreas departamentales:
El cliente demanda información de cada departamento y quiere tener un único interlocutor.
c) La utilización del comercio electrónico:
Hay que asegurar las transacciones entre cliente y proveedor y permitir que miles de usuarios entren a nuestros servidores a la búsqueda de información.
d) La multiplicidad de usuarios y dispositivos:
El número de internautas se va a incrementar exponencialmente con tecnologías como ADSL o 4G.

e) La Conectividad permanente**:** Internet es conectividad permanente 24 x 365. No vale apagar los servidores cuando se cierra la oficina.

La protección perfecta no existe, ningún modelo puede resolver todos los problemas de seguridad. En relación con la seguridad en redes se pueden postular varios planteamientos:

1) Ninguna seguridad

La medida más simple posible es no hacer ningún esfuerzo en seguridad y tener la mínima, cualquiera que sea, por ejemplo la que proporcione el vendedor de forma preestablecida. Se supone que este no es un modelo a seguir.

2) Seguridad a través de ser desconocido

Con este planteamiento se supone que un sistema es seguro sólo porque nadie sabe de él. Depender de la seguridad de ser desconocido no es una buena opción.

3) Seguridad para anfitrión

El modelo plantea reforzar la seguridad de cada máquina anfitrión por separado, y hacer todo el esfuerzo para evitar o reducir los problemas de seguridad que puedan afectar a ese anfitrión específico.

Un modelo de seguridad para anfitrión puede ser apropiado para sitios pequeños o con necesidades de extrema seguridad. La seguridad para anfitrión es un mecanismo costoso que implica mucha dedicación y restricciones, pero de hecho, todos los sitios deben incluir algún nivel de seguridad para anfitrión en sus planes de seguridad.

4) Seguridad para redes

Conforme los entornos se hacen más grandes y diversos, es más difícil asegurar anfitrión por anfitrión, por ello ahora se tiende hacia un modelo de seguridad para redes. Las medidas de seguridad para redes incluyen la instalación de *firewall´s* para proteger los sistemas y redes internas, la utilización de estrictas medidas de autenticación y el uso de encriptación para proteger los datos que transitan por la red. Un solo *firewall* puede proteger cientos o miles de máquinas contra un ataque, pero debe ser complementado con alguna medida de seguridad para anfitrión de las máquinas individuales.

La seguridad de las redes requiere un enfoque global, distribuido y completo. La sola incorporación de dispositivos cortafuegos (*firewall*), no garantiza la seguridad de la información, por lo que su implementación debe ser parte de un conjunto de medidas dentro de una política de seguridad global y particular de cada organización o empresa.

6.1. AMENAZAS Y ATAQUES A LAS REDES DE ORDENADORES

Se entiende por amenaza una violación potencial de la seguridad de un sistema y por ataque la materialización de una amenaza.

Atendiendo a su origen, las amenazas se pueden clasificar en involuntarias e intencionadas. La mayor parte de los desastres no son intencionados, son accidentes o equivocaciones.

Según la arquitectura de seguridad OSI, por la forma de actuación las amenazas intencionadas y los ataques derivados se pueden clasificar en pasivas y activas:

1. Las amenazas pasivas atentan contra la confidencialidad de la información, y su rasgo distintivo es que no alteran el estado de ésta ni del sistema en su conjunto.

El caso proverbial de amenaza pasiva es la interceptación (coloquialmente pinchazo) de un canal de comunicación para aprehender ilegítimamente los datos que por él circulan, sea en claro o cifrados. El prototipo de ataque de interceptación de datos es el producido por un

sniffer, dispositivo *hardware o software* que captura toda la información que atraviesa un enlace.

Los ataques pasivos son difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible minimizar su efecto mediante el cifrado de la información.

Aunque la información que transite por la línea de comunicación vaya cifrada, y por tanto no sea posible para un intruso averiguar el contenido de los mensajes transmitidos, puede leer las cabeceras de los paquetes, donde puede encontrar la identidad y situación de los nodos y a partir de aquí, registrando la dirección, el momento, la frecuencia, la longitud, etc. de los citados mensajes, vaticinar la naturaleza de los mismos. Esta interceptación es más sutil que la anteriormente expuesta, y recibe el nombre de análisis del tráfico (*traffic analysis).*

2. Las amenazas activas provienen de la conexión de dispositivos específicos, a la línea de transmisión, para alterar o borrar señales o generar otras nuevas. Los ataques activos cambian el estado del sistema, por lo que son más fácil detectar que los pasivos. Usualmente se distinguen tres tipos de amenazas activas: interrupción, modificación y generación.

a) La interrupción

Es una amenaza a la disponibilidad de la información y consiste en provocar la falta de continuidad de la transmisión o de un proceso. En un caso extremo, puede consistir en la destrucción del hardware o software, o bien un corte de la línea física de comunicación. Amenazas más elaboradas que los anteriores son la supresión de los mensajes con un cierto destino o la saturación de un servicio mediante numerosas y reiteradas peticiones al mismo. Una amenaza de este tipo es la que se conoce como denegación de servicio.

b) La modificación

Es una amenaza a la integridad de la información, que consiste en la alteración fraudulenta de mensajes (en el caso de redes) o en general de cualquier información, por ejemplo, cambios no autorizados en programas o datos. Un caso frecuente en redes es la suplantación de un usuario por otro cambiando las cabeceras de los mensajes IP de aquel, lo que se denomina *IP spoofing.*

c) La generación

Consiste en la construcción de mensajes falsos que se hacen pasar por verdaderos. Un ejemplo es la replicación de un mensaje, consistente en la captura del mismo para su posterior emisión tantas veces como se considere oportuno. Dentro de este tipo se encuentra el *IP hijaking.*

Aunque los ataques activos son fáciles de detectar, es muy complejo evitarlos de una manera absoluta ya que sería necesario proteger, debidamente y en cualquier momento, todos lo recursos de la organización. Para los ataques pasivos es más importante la prevención que la detección. Sin embargo, si no ha sido posible evitar el ataque, es fundamental su detección y la recuperación de cualquier situación anómala que haya podido ocasionar.

6.2. AMENAZAS PROGRAMADAS

Se entiende por amenaza programada cuando las instrucciones de un programa se diseñaron con la intención de hacer daño.

Existen muchos y diferentes tipos de amenazas programadas. La ocurrencia de estas amenazas ha sido descrita casi uniformemente por los medios de comunicación de masas como virus. La mayoría de los expertos efectúan la siguiente clasificación práctica de programas maliciosos:

a. Herramientas de seguridad. Las herramientas de seguridad están diseñadas para detectar problemas de seguridad y reportarlos a los expertos para que los corrijan. Estas herramientas también las usan los agresores que buscar fallas de seguridad y comprometer los sistemas o las redes.
b. Puertas traseras. Las puertas traseras son piezas de código escritas dentro de aplicaciones o sistemas operativos para facilitar a los programadores el acceso a programas sin tener que pasar por los medios normales de autenticación. La puerta trasera es un código que reconoce alguna secuencia especial de entrada, o que se dispara al ejecutarla desde un determinado número de identificación de usuario, otorgando entonces el acceso especial. Las puertas traseras se convierten en amenazas cuando las usan programadores sin escrúpulos para lograr accesos no autorizados. Algunas veces, un intruso inserta una puerta trasera después de haber penetrado en un sistema, convirtiéndose en root para posteriormente volver a entrar con toda facilidad e impunidad.
c. Bombas lógicas. Las bombas lógicas son amenazas que permanecen latentes por un extenso periodo hasta que se disparan, en ese momento, ejecutan una función que no es la función propia del programa en el cual están contenidas.
   Un tipo especial de bombas lógicas son las que se usan para controlar los tiempos de cobertura y forzar pagos u otras provisiones de contratos. Estas bombas hacen que se detenga el programa al pasar una determinada fecha o periodo a menos que se tome una acción especial.

d. Caballos de Troya. Análogos al originario de su nombre, los caballos de Troya modernos son programas que parecen hacer lo que el usuario espera que hagan, pero realmente están haciendo algo más sin su conocimiento.
e. Virus. Un virus es una secuencia de código que se inserta en otro código ejecutable, para que cuando el programa regular se ejecute, el código viral también se ejecute. Los virus no son programas independientes, no pueden ejecutarse por si solos, necesitan que se ejecute el programa que los hospeda para activarlos. Un virus típico pasa por las fases de nacimiento, latencia, activación (ocultamiento, reproducción, infección y activación) y erradicación.
f. Gusanos (“worms”). Los gusanos son programas que se pueden ejecutar independientemente y viajar de máquina en máquina (nodo) a través de las conexiones de red; los gusanos pueden hacer que porciones de ellos mismos se ejecuten en muchas máquinas diferentes. Los gusanos utilizan las redes para propagarse de un sistema a otro. Una vez dentro pueden comportarse como un virus o un caballo de Troya. Para propagarse pueden utilizar el correo electrónico, realizar una ejecución remota o un login remoto.
   Un gusano pasa por las mismas fases que un virus: latencia, propagación y activación

Los gusanos son difíciles de escribir, pero pueden causar mucho daño. Desarrollar un gusano requiere conocer y estar familiarizado con las facilidades y servicios de red, y con las facilidades operativas requeridas para soportarlos una vez que han alcanzado una máquina. Si existe la sospecha de que, a través de la red, una máquina está bajo el ataque de un gusano se recomienda, además de analizar el problema por un experto en seguridad en redes, cortar inmediatamente las conexiones de red para evitar que se propague.

g. Bacterias. Las bacterias son programas que explícitamente no dañan ningún fichero, su único propósito es replicarse.

Un programa bacteria típico ejecuta dos copias de sí mismo simultáneamente en sistemas de multiprogramación, o quizás crea dos archivos nuevos, cada uno de los cuales es una copia del archivo fuente original del programa bacteria. Esos dos programas a su vez pueden copiarse a sí mismos dos veces, y así sucesivamente. Las bacterias se reproducen de forma exponencial, eventualmente ocupando toda la capacidad del procesador, la memoria o el espacio en disco, negando el acceso a los usuarios a esos recursos. Los sistemas operativos sin cuotas ni límites de recursos son especialmente susceptibles a este tipo de ataques.

Un agresor puede insertar instrucciones dañinas en otros lugares además de en los programas precompilados. Los archivos de interprete de instrucciones awk, Perl, guiones CGI (Common Gateway Interface), Active X, archivos PostScript. Es importante señalar que la creciente popularidad de los navegadores y de los servidores web propicia que los virus y los caballos de Troya puedan desarrollarse y propagarse. Este ambiente incluye:

- Los ficheros *PostScript* que son transferidos vía FTP o web y automáticamente interpretados pueden contener instrucciones dañinas.
- Las páginas web que contienen *applets* en lenguajes como Java que se bajan y ejecutan en el cliente. Algunos de estos lenguajes permiten que los *applets* abran conexiones de red con máquinas arbitrarias, para generar otros procesos y modificar archivos.
- El correo codificado en MIME puede contener archivos diseñados para sobrescribir archivos locales o contener aplicaciones codificadas que, cuando se ejecutan, realizan actos maliciosos, incluyendo el reenvío del mismo código malicioso en otro mensaje.

Para protegerse de las amenazas programadas se pueden seguir, entre otras, las siguientes recomendaciones:

- Verificar regularmente la integridad de los archivos importantes.
- Revisar los programas nuevos, especialmente los de fuentes desconocidas, y ante cualquier sospecha no deben usarse. Si es posible primero instalarlos en algún sistema para pruebas, para aislar problemas e identificar incompatibilidades.
- Aceptar solamente programas de fuentes confiables.
- No confiar automáticamente en los programas de firmas o grupos comerciales. Algunas firmas comerciales insertan puertas traseras en su código para permitir mantenimiento o recuperar contraseñas perdidas.
- Pedir garantías y responsabilidades por escrito del código que se compra e instala.
- Hacer regularmente copias de respaldo de la información crítica para que, si algo pasa, se pueda restaurar la información y el sistema.
- No ejecutar nada como *root/Administrador* excepto cuando sea totalmente imprescindible.
- Tener instalado y actualizado un programa antivirus.

Como ya hemos comentado, en algunos casos, estos segmentos de programas se usan para actuaciones lícitas. Por ejemplo, los gusanos pueden usarse para hacer cálculos distribuidos en procesadores ociosos; las puertas traseras son útiles para depurar programas, las bombas lógicas se usan para controlar los tiempos de cobertura de licencias de uso y los virus pueden escribirse para actualizar código fuente y parches para errores. El propósito, no el enfoque, es lo que hace que una amenaza programada sea peligrosa.

6.3. ESTRATEGIAS DE SEGURIDAD EN REDES

Hay que recalcar que el primer factor para la protección de los sistemas de red, es implantar una buena política de seguridad, hacerla cumplir, revisarla y tenerla actualizada.

Antes de establecer cualquier medida de seguridad, es importante comprender algunas estrategias básicas empleadas para la protección de un sitio:

Defensa a fondo

Instalar varios mecanismos que se respalden entre sí, no depender solamente de un mecanismo de seguridad, sin importar cuán fuerte parezca. El fallo de un solo mecanismo de seguridad no debe comprometer toda la seguridad. Aplicaciones de este principio se pueden ver en otros aspectos de la vida, por ejemplo, es probable que la puerta de acceso a nuestra vivienda tenga más de una cerradura, un cerrojo o una barra.

Cualquier seguridad puede ser violada por atacantes dispuestos a asumir suficientes riesgos y emplear suficiente recursos. El objetivo es que el intento de violación sea arriesgado o costoso para los atacantes, esto se puede alcanzar adoptando múltiples mecanismos que se den respaldo y redundancia entre sí: líneas de back-up, un firewall para la seguridad de red, restricción de acceso al anfitrión bastión; complementadas con otras medidas como educación de los usuarios, administración cuidadosa del sistema, etc.

Punto de choque

Un punto de choque obliga a los atacantes a utilizar un canal angosto que se puede monitorizar y controlar. Hay muchos ejemplos de puntos de choque en la vida cotidiana: la caseta de un paso fronterizo, las cajas registradoras en un supermercado, la taquilla de un cine.

En la seguridad de redes, el firewall entre un sitio e Internet (suponiendo que es la única conexión entre ambos) es un punto de choque; cualquiera que vaya a atacar ese sitio desde Internet tendrá que pasar a través de ese canal, el cual debe estar defendido contra los ataques y estar listo para responder si los detecta.

El eslabón más débil

Una cadena es tan fuerte como su eslabón más débil. Se deben conocer los puntos débiles de las defensas para si es posible eliminarlos y si no monitorizarlos con cuidado.

Postura de falla segura

En la medida de lo posible, los sistemas deben tener una *falla segura*, es decir, si van a fallar deben hacerlo de tal forma que nieguen el acceso a un atacante en lugar de dejarlo entrar.

La mayoría de los mecanismos que se utilizan en la seguridad en redes son de falla segura. Si un enrutador para filtrado de paquetes no funciona, no deja pasar ningún paquete. Si un programa proxy falla, no proporciona servicio.

Participación universal

Para que sean efectivos, la mayoría de los sistemas de seguridad requieren de participación universal (o por lo menos ausencia de oposición activa) de todo el personal de un sitio. Si alguien opta por salirse de los mecanismos de seguridad, entonces un atacante puede agredir al sitio a través del acceso de esa persona.

Diversificación de defensa

Si todos los sistemas son iguales, alguien que sepa entrar a alguno de ellos quizá penetre a todos.

La idea es utilizar sistemas de seguridad de diferentes proveedores para reducir las posibilidades de un problema o error de configuración común que pueda comprometerlos a todos. Sin embargo, hay un balance en términos de complejidad y costo, instalar varios sistemas diferentes es más difícil y requiere más esfuerzo que instalar un solo sistema (o incluso varios sistemas idénticos).

Hay que tener cuidado con la diversidad ilusoria. Por ejemplo, sólo por utilizar sistemas UNIX de diferentes proveedores no se consigue diversidad, pues la mayoría de ellos derivan del código fuente de BSD o *System* V.

También hay que tener en cuenta que diversos sistemas configurados por la misma persona (o por el mismo grupo de personas) pueden compartir problemas comunes. Si el problema es un malentendido sobre cómo funciona un protocolo específico, todos sus sistemas pueden estar configurados incorrectamente, ya que se configuraron de la misma forma, siguiendo ese malentendido.

Simplicidad

La simplicidad es una estrategia de seguridad por dos razones:

- Las cosas sencillas son más fáciles de comprender; si algo no se entiende no se puede saber si, en realidad, es seguro o no.
- Lo complejo proporciona muchos escondites que permiten ocultar toda clase de cosas.

Ante la mayoría de las cuestiones planteadas hay dos posturas fundamentales que se pueden adoptar con respecto a decisiones y políticas de seguridad:

1) Postura de negación preestablecida:

"Lo que no está permitido expresamente está prohibido. Especificar sólo lo que se permite y prohibir todo lo demás".

La postura de negación preestablecida es una postura de falla segura, se basa en que lo desconocido *puede* dañar. Es la opción obvia más segura para los responsables de seguridad pero en general no es bien aceptada por los usuarios. Para determinar lo que se va a permitir, se debe:

- Examinar los servicios que necesitan los usuarios.
- Considerar cómo afectarían a la seguridad tales servicios y cómo se pueden proporcionar de manera segura.
- Permitir sólo los servicios que se comprenden, que se pueden proporcionar con seguridad y para los cuales se ve una necesidad legítima.

2) Postura de permiso preestablecido:

"Lo que no está prohibido expresamente está permitido. Especificar sólo lo que se prohíbe y permitir todo lo demás".

La mayoría de los usuarios y administradores prefieren la postura de permiso preestablecido. Tienden a suponer que todo estará, por omisión, permitido, y que se irán prohibiendo ciertas acciones y servicios problemáticos específicos conforme sea necesario.

Los usuarios quieren que se les diga qué es peligroso; que se enumeren esas pocas cosas que, según ellos, no pueden hacer y que se les deje hacer todo lo demás.

Esta postura, parte de que a priori se conocen y de manera precisa cuáles son los peligros específicos, cómo explicarlos para que los usuarios los comprendan y cómo protegerse contra ellos. Adivinar qué peligros podría haber en el sistema o en Internet es, en esencia, una tarea imposible. Si no sabe que algo es un problema, no estará en la lista de "prohibido". En ese caso, continuará siendo un problema hasta que se den cuenta de ello, y es probable que se percaten porque alguien se aprovecha de él.

6.4. SEGURIDAD EN INTERNET

Internet significa literalmente "redes interconectadas", por tanto, no es una red única, como popularmente se cree, sino una enorme colección de miles de redes de ordenadores más pequeñas conectadas entre sí a lo largo de todo el mundo. Por esto, Internet es conocida también como la Red de redes.

La conexión entre las diferentes redes que constituyen Internet se diseñó de forma transparente al usuario, su estructura interna queda oculta al usuario final y de aquí proviene el hecho de que se confunda a Internet con una única red de ordenadores.

Internet nació como una serie de redes que promovían el intercambio de información entre investigadores que colaboraban en proyectos conjuntos o compartían resultados usando los recursos de la red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación especial por la confidencialidad de los datos ni por ninguna otra problemática de

seguridad. Estaba totalmente desaconsejado usarla para el envío de documentos sensibles o clasificados.

Los protocolos de Internet fueron diseñados de forma deliberada para que fueran simples y sencillos. El poco esfuerzo necesario para su desarrollo y verificación jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser echados en falta.

La conexión del mundo empresarial a Internet se ha producido a un ritmo vertiginoso muy superior a la difusión de cualquier otra tecnología anterior. Ello ha significado que esta Red de redes se haya convertido en el medio más popular de interconexión de recursos informáticos y embrión de las anunciadas autopistas de la información.

La expansión de Internet ha modificado la forma de comunicación de empresas y organizaciones. Internet no sólo ha abaratado costes de comunicación, también está ofreciendo una ventaja más significativa; la interconexión "global". La utilización de Internet como canal comercial, pasa realmente por la resolución de los problemas de seguridad.

Al amparo de Internet han aparecido dos estructuras similares, las Intranets y las Extranets:

- Una Intranet es una Internet interna esto es, privada, se trata de una LAN basada en TCP/IP. Esta puede estar conectada o no con Internet, pero cuando lo está lo hace a través de un cortafuegos que permite que desde fuera de la Intranet solo se vea lo que sus administradores hayan previsto que se vea. El concepto de Intranet es de una importancia creciente ya que cada vez más organizaciones y empresas, a la vista del éxito de Internet, adoptan los protocolos TCP/IP y los estándares de Internet en sus redes para explotar su propia información.
- Si una Intranet es una LAN basada en TCP/IP, una Extranet es una WAN basada en TCP/IP que funciona sobre Internet.

Se ha incrementado la variedad y cantidad de usuarios que usan la red para los fines más diversos: el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, el comercio, la cooperación altruista, la práctica política, el ocio,… En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas. *Hackers, Whitehats, crakers, sniffers…*

6.5. DISEÑO DE LA ARQUITECTURA DE SEGURIDAD EN INTERNET

Para garantizar la seguridad en redes se pueden distinguir dos tipos de medidas complementarias, encaminadas a conseguir:

Protección de los accesos.

El paradigma de éste tipo de medidas es la instalación de un cortafuegos *(firewall)* que defiende el acceso a una parte protegida de una red.

Los cortafuegos son mecanismos que permiten filtrar los accesos, en función de diferentes criterios o parámetros, determinando quien puede y quién no puede acceder de dentro a fuera y viceversa.

Las técnicas que utilizan los "*firewalls*" son una combinación de:

- Filtrado de paquetes, determinan que paquetes pueden salir y/o entrar en la red
- Filtrado a nivel de aplicación, controlan parámetros específicos para cada conexión: momento de llamada, número de sesiones, identificativos del que llama y del llamado, tipo de servicios requeridos,...

Aplicaciones seguras extremo a extremo.

Si pensamos por ejemplo en correo electrónico consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado, cifrado, previo al envío, de forma que este mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos.

En el diseño de la Arquitectura de Seguridad en Internet se debe realizar una selección de los mecanismos y controles necesarios para conseguir el nivel de seguridad establecido en el análisis de riesgos. Entre los mecanismos que podemos contar cabe señalar los siguientes:

Sistemas Operativos Seguros:

Instalación de sistemas operativos compatibles, pero específicamente diseñados para impedir y contener posibles ataques de seguridad, que integren, en ellos, las aplicaciones: web, mail, etc.

Sistemas de Seguridad Perimetral:

Implantación de cortafuegos para la seguridad perimetral, que incluyan:

- El bastionado de sistemas: Para minimizar el riesgo de vulnerabilidades y acceso no autorizado, en esos sistemas sólo se ejecute lo que es estrictamente necesario para el desarrollo de la función específica.
- Sistemas de *WebProxy*: Configuración de un servidor con sistema operativo virtual como interlocutor/proxy entre servidores y clientes de Internet, que contemple mecanismos de Single-Sign-On para el control de acceso y autorizaciones con contraseña única
- Redes Privadas Virtuales (VPN): Implantación de protocolos y sistemas que gestione adecuadamente los aspectos de confidencialidad e integridad de la información transferida y garanticen la autenticación y autorización de los usuarios.
- Sistemas de Antivirus Corporativos: Implantación de sistemas antivirus corporativos, que incluyan el control del perímetro, los puestos de trabajo, el correo electrónico y los sistemas de ficheros.
- Infraestructura de Clave Pública (PKI): Implantación de la infraestructura de clave pública, para la gestión de certificados digitales, y definición de la Política de Certificación.