Ingeniería en Desarrollo de Software
Semestre 6

Programa de la asignatura:
Interconectividad de redes

Unidad 3. Seguridad de redes

Ciudad de México, noviembre del 2023

Clave:
15143634

Universidad Abierta y a Distancia de México

Índice

Unidad 3 Seguridad de redes

Presentación de la unidad

En esta tercera unidad se abordarán temas de seguridad de redes tales como mecanismos y políticas de seguridad. Es importante que conozcas este tema porque, mediante ellos, es posible mantener los sistemas informáticos y las redes seguras.

Como recordarás, mediante las redes se transmite información, la cual puede ser muy especial o confidencial. Si no se cuentan con las políticas o la tecnología necesarias, la red podría sufrir ataques (entiéndase cualquier intervención ajena a los sistemas informáticos o de comunicaciones de una empresa), que pueden resultar en corrupción dela información y degradación de servicios. Dichos ataques podrían poner en riesgo la información, ya sea de la empresa donde se encuentre instalada una red, o la información personal de los usuarios.

En esta unidad se explicarán las prácticas de seguridad más comunes, con el fin de que puedas apoyar en la toma de decisiones sobre su implementación en tus desarrollos de software; por ejemplo, lo más común en un sistema es *proteger* su acceso mediante una contraseña, la cual debe viajar de manera segura a través de una red; es decir, encriptada (encriptar es, de alguna manera, esconder la contraseña para que, cuando viaje a través de la red, sea difícil de leer para alguien que desee interceptar los mensajes), y de esta forma garantizar la seguridad en el acceso y la transmisión de información mediante las redes.

Logros

Al término de esta unidad lograrás:

- Identificar las diferentes tecnologías de encriptación.
- Identificar las técnicas de seguridad de una red.
- Relacionar los mecanismos de seguridad con los requerimientos de administración de red.
- Realizar el diseño e implementación de redes en un caso particular.

Competencia específica

- Configurar una interconectividad de redes de área extensa para determinar los métodos de seguridad, a partir de los requerimientos específicos.

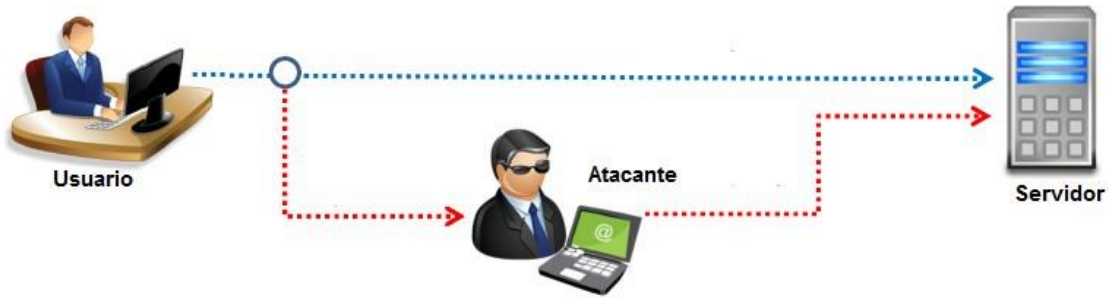
3. Seguridad de redes

> *Las redes informáticas y entre ellas Internet, son uno de los mayores peligros que existenen la seguridad de un sistema informático, ya que actualmente la mayoría de las amenazas yataques provienen del exterior a través de la red* (García y Alegre, 2011, p. 45).

La única manera de tener segura la información de un equipo de cómputo es no conectándolo a ninguna red, pero esto no haría nada funcional a ese equipo de cómputo, los recursos a los cuales podría acceder y compartir serían muy limitados. Las redes informáticas, al dar interconectividad a diversidad de equipos, se vuelven inseguras ya que existen muchas personas accediendo a la red para intercambiar información; como muchas de estas personas tienen poco o nulo conocimiento de informática en general, son un blanco fácil para atacar.

La seguridad de redes nace de la misma inseguridad que se genera en las redes; inseguridad que se crea, a veces, con el simple hecho de poner contraseñas sencillas, no configurar correctamente un equipo de cómputo, o que al instalar un software no se personalice adecuadamente, etcétera. La seguridad de redes es parte de algunas otras áreas de especialización dentro de la seguridad de la información; las cuales, según Areitio (2008) son:

- **Gestión de seguridad:** se refiere al establecimiento de políticas y procedimientos informáticos que instituye la alta dirección de una empresa.
- **Seguridad de las operaciones**: establece controles de identidad, audita y monitoriza accesos a equipo de red y de cómputo.
- **Gestión de riesgos**: da respuesta y recuperación a la gestión de riesgos, los identifica, prioriza y, con base en ello, establece tiempos de respuesta y de recuperación en caso de desastre.
- **Seguridad en redes y telecomunicaciones**: asegura la red utilizando equipos de red; por ejemplo, firewalls, o con protocolos seguros tales como https en vez de http. Como recordarás, la diferencia entre ellos es la palabra *secure.* Ambos protocolos tienen las siglas http, *Hypertext Transfer Protocol*, que en español es *protocolo de transferencia de hipertexto.* El *hipertexto* es lo que se conoce como links de Internet. En el protocolo https, la palabra *secure*, indica que permitirá la transferencia segura de hipertexto, a través de algoritmos de encripción.
- **Criptología:** técnica mediante la cual se cifra, descifra, se firma digitalmente, se ocultan ficheros y mensajes mediante un proceso llamado esteganografía.



Esquema de un ataque. Fuente: Secur-IT @C.R.S, 2011b.

En el esquema anterior se muestra un típico **ataque** a la información de un usuario que se conecta a un servidor. Se observa que el atacante está en medio del usuario y del servidor. Es común que el atacante esté observando todo lo que el usuario envía al servidor; en algunos casos puede hacerse pasar por el usuario. En todos los casos obtiene información o se hace pasar por otra persona para sacar más información o algún provecho. Para mitigar esto, se puede hacer uso de una red privada virtual o **VPN** (*Virtual Private Network),* una VPN no tiene que ser forzosamente conectada con una red empresarial. Actualmente existen diversidad de servicios de VPN que ofrecen privacidad al enviar la información o recibirla. En el caso de tener una VPN, un atacante deberá de **descifrar** toda la información que recibe, ya que cifrada no le sirve de nada y, por tanto, no podrá perjudicar al usuario. El tema de cifrado se verá más adelante, sólo se hizo la aclaración para que notes la importancia de la seguridad en las redes y en los sistemas informáticos.

En la presente unidad se revisarán aspectos de **seguridad** tales como la **criptografía** y **esteganografía**, firmas, certificados digitales y políticas de seguridad que permiten hacera las redes más seguras.

3.1. Introducción a la seguridad

La seguridad de redes forma parte de la seguridad en sistemas de información, pues es información finalmente lo que se envía a través de las redes.

El ámbito de la aplicación de seguridad de los sistemas de información abarca el desarrollo, la operación, la administración y el mantenimiento de sistemas y aplicaciones (Areitio, 2008).

De manera muy vertiginosa, las redes informáticas han adquirido mayor tamaño y mayor importancia. Si la seguridad de la red se ve afectada habría consecuencias graves, tales como la pérdida de privacidad o el robo de información. Aunado a esto, y para hacer más

compleja la situación, las amenazas potenciales a la seguridad de las redes informáticasse encuentran siempre en evolución (Cisco, 2013b).

A medida que el comercio electrónico y las aplicaciones de Internet siguen creciendo, es muy difícil encontrar el equilibrio entre estar aislado y abierto. Además, el aumento del comercio móvil y de las redes inalámbricas exige soluciones de seguridad perfectamente integradas, más transparentes y más flexibles (Cisco, 2013b).

Como puedes observar, la seguridad de las hoy llamadas tecnologías de la información y de la comunicación (TIC), es muy importante. Como futuro Ingeniero en Desarrollo de Software, es algo que no debes dejar pasar por alto a la hora de desarrollar, probar y echar a andar una aplicación en un entorno, ya sea Intranet o Internet.

3.1.1. Definición

La tendencia, cada vez más dominante, hacia la interconectividad e interoperabilidad de redes, de los equipos de cómputo (PC, lap top, smartphones) y de las aplicaciones que utilizan las organizaciones ha situado a la seguridad de los sistemas de información como un elemento central en el desarrollo de la sociedad (Areitio, 2008).

Pero, ¿qué es la seguridad informática? Según Cervigón y García (2011) "la seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo" (p. 2).

La seguridad informática implica las **políticas**, **estándares** y **procedimientos** usados para mantener segura la información. Para ello es necesario considerar los objetivos principales de la seguridad, los cuales, según Areitio (2008, p. 3) son:

1. Disponibilidad y accesibilidad de los sistemas y datos, sólo para su uso autorizado
2. Integridad
3. Confidencialidad de datos y de la información del sistema
4. Responsabilidad a nivel individual (registros de auditoría)
5. Confiablidad

A continuación, se explicará a detalle cada uno de los puntos anteriores.

1. Disponibilidad y accesibilidad de los sistemas y datos, sólo para su uso autorizado: los sistemas informáticos deben estar disponibles y accesibles para los usuarios con acceso autorizado. La disponibilidad y accesibilidad a un sistema informático

la proporciona el administrador de dichos recursos. En la práctica es muy difícil proporcionar una disponibilidad del 100% a los sistemas y a los datos, ya que los sistemas, por ejemplo, se encuentran en equipos físicos que se alimentan de energía eléctrica, y el suministro de ésta escapa al control de los administradores de un sistema informático. Aunque el recibo de luz se pague mes con mes, no es posible controlar que un día el suministro se vea interrumpido, tal vez por una sobre carga a la planta. Otra razón por la que es difícil garantizar una disponibilidad del 100% de los sistemas y de los datos, se debe a la posibilidad que una red se interconecte con redes ajenas, lo cual tampoco es posible controlar, pero aun cuando sea complicado ofrecer una disponibilidad del 100%, se deberá trabajar para que la disponibilidad sea muy cercana a este número. Los accesos autorizados a un sistema se refieren comúnmente a los de tipo **controlado**; por ejemplo, utilizando un nombre de usuario y una contraseña o *password.*

2. Integridad: garantiza que la información no haya sido alterada por un tercero y que **llegue** a su destino en forma **íntegra;** es decir, tal como el usuario envía la información la recibirá el usuario receptor, la integridad debe observarse en dos ámbitos:

- **Integridad de datos:** indica si los datos han sido **alterados** de forma no autorizada mientras se procesan, almacenan o transmiten. Según Stallings (2004) la integridad de los datos se refiere a "la seguridad de que los datos recibidos son exactamente como los envió una entidad autorizada (no contiene modificación, inserción, omisión, ni repetición)" (p. 10). Comúnmente, para verificar esta propiedad existen herramientas que escanean la información y generan, de acuerdo con el tamaño y al tipo de archivo, un **código** al que se le denomina **hash.** Se debe verificar que coincida con el otro hash que se crea cuando se almacena, o antes de transmitir.
- **Integridad del sistema**: es la cualidad que posee un sistema cuando realiza sus funciones de manera normal, sin ser manipuladas por un tercero que no esté autorizado.

3. Confidencialidad de datos y de la información del sistema: es requisito indispensable que los datos y la información de un sistema sean privados y que no puedan ser leídos por usuarios no autorizados. La diferencia entre integridad y confidencialidad radica en que la primera se refiere a que no haya sufrido cambios la información, mientras que la segunda a que la información no sea visible para quien no va dirigida.

4. Responsabilidad a nivel individual (registros de auditoría): es la capacidad que debe tener un sistema de guardar registros por cada usuario que se conecte a un sistema, esto con el fin de llevar bitácoras de uso para detectar anomalías de uso.

5. Confiabilidad: es el aseguramiento de que existen las políticas adecuadas paraproteger la información y los datos. En caso de desastre debe existir un plan de recuperación.

Para que exista **disponibilidad y acceso a los sistemas y datos** muy cercanos al 100%, deben existir las condiciones de seguridad (acceso a usuarios a los sistemas) y de infraestructura (red y energía de los equipos que proporcionan los servicios) necesarias.
Para que exista **integridad de datos**, deben existir métodos o procedimientos que permitan que no se corrompan los datos; por ejemplo, restringir el acceso mediante algunos datos confidenciales como el nombre de usuario y la contraseña o *password,* de manera tal que sólo los usuarios que legítimamente dispongan del acceso puedan hacer uso de él. Para la **confidencialidad de datos** se pueden usar métodos como encriptación o esteganografía, los cuales se revisarán en el siguiente subtema, para este momento basta con saber que **encriptar** es **ocultar** la información siguiendo un código, mientras que **esteganografía** es ocultar la existencia de un mensaje, más no su contenido. Para los **registros de auditoría** es altamente recomendable habilitar el registro de logs de los sistemas de cómputo o de red que se desean proteger. Los **logs** son las bitácoras de los sistemas en donde se guarda la información de determinados eventos; por ejemplo, existen logs de aplicaciones, de sistema, de usuarios, etcétera. La **confiabilidad** existe cuando estas u otras prácticas de seguridad se han puesto en marcha, y ayudan al administrador del sistema informático o de comunicación a contar con sistemas más confiables.

3.1.2. Criptología y esteganografía

La importancia de la *criptología* se ilustra en el siguiente ejemplo de aplicación. Supongamos que dos países en guerra envían mensajes entre sus aliados con el fin de **transmitir** un mensaje de ayuda, ¿Qué pasaría si éste fuera interceptado por fuerzas enemigas y, peor aún, que el mensaje fuera fácilmente leído por el enemigo? Muchos países a quienes se interceptan los mensajes son vencidos, porque el enemigo tenía información sobre él, **información** muy importante, o como se dice actualmente, información de **seguridad**. Este es uno de los ámbitos de aplicación de la criptografía y la esteganografía ya que, en este ejemplo, se hace necesario que los mensajes que se transmitan entre personas y países no sean leídos por nadie más, sólo por el legítimo destinatario.

La **Criptología** es el estudio de los sistemas de comunicaciones secretas. Está constituida por dos campos de estudio complementarias entre sí (Sedgewick, 1992).

Criptografía: técnica utilizada para **ocultar** la información de manera tal que, un usuario que no conozca las claves para desencriptarla no pueda acceder a la información (García y Alegre, 2011). Este tema se revisará más adelante.

Criptoanálisis: estudio de las formas de transgredir los sistemas de comunicación secretas (Sedgewick, 1992).

Por su parte, la **esteganografía** es la ciencia que estudia los procedimientos encaminados a ocultar la existencia de un mensaje, en lugar de ocultar su contenido (MMC, 2007). "La palabra esteganografía significa escritura oculta" (Ramos y Ribagorda,2004, p. 418).

Con base en las definiciones anteriores, es posible decir que la *criptología*, a través de la criptografía, se encarga de **evitar** que una persona diferente al destinatario original pueda leer un mensaje; esto lo hace a través de algoritmos de encriptación o algoritmos de cifrado, los cuales se revisarán más adelante. Mientras que la *esteganografía* no pretende encriptar el mensaje; lo que pretende es ocultar el contenido de la información sino más bien ocultar todo el mensaje, es decir, la criptología mediante la criptografía oculta el contenido del mensaje, se observa que hay un mensaje, pero no se puede leer, porque se activa un mecanismo mediante el cual se oculta, mediante la esteganografía se oculta el mensaje y como se oculta no se sabe de su existencia y por ende el contenido nadie lo veal no saber que existe un mensaje.

La *esteganografía* consiste en ocultar la existencia de información en un canal de transmisión. La criptografía, por su parte, cifra o transforma un mensaje en otro. Se sabe que hay un mensaje. De esta manera, la esteganografía jamás transforma el mensaje original, sólo lo mantiene **oculto** (Ramos y Ribagorda, 2004). Por mensaje debe entenderse, en el ámbito de la aplicación de la criptología y esteganografía, cualquier dato que viaja a través de las redes. Un usuario y un *password* también son mensajes por que viajan a través de una red.

Ahora te preguntarás y **¿De qué manera se oculta un mensaje?** Con el auge de la informática, el mecanismo estenográfico más extendido está basado en imágenes digitales. Se sustituye el bit menos significativo de cada byte por los bits del mensaje que se desea ocultar. Dado que casi todos los estándares gráficos tienen una mayor graduación de colores de los que el ojo humano puede apreciar, la imagen no cambiará de apariencia de forma notable. Esta no es la única manera de esconder un mensaje, se puede esconder en archivos de video, de música o hasta en el mismo formato de texto (Moliner, 2005).

De una manera muy sencilla se puede ocultar un mensaje, se expondrá un ejemplo a continuación:

Si se cuenta con un archivo de texto en una computadora y en él se tiene, por ejemplo, una agenda telefónica, se puede decir que el contenido del archivo de texto es el mensaje. Ahora bien, si se observa la extensión del archivo de texto seguramente será .txt; esto indica al sistema operativo que, efectivamente, se trata de un archivo de texto y, por lo tanto, cuando se realice la acción para abrir el archivo, el sistema operativo intentará abrirlo con un editor de texto. El sistema operativo asocia cada extensión de archivo con un programa en especial, de manera tal que cuando el usuario haga doble clic se abrirá con el visor predeterminado para ello. Ahora reflexiona: ¿Qué pasaría si un archivo con extensión .txt se cambia a .jpg (muy usada en las fotos)? Al intentar abrir el archivo y ver el contenido, el programa mostrará un mensaje de que está corrupto, pero realmente no es así, simplemente que el programa visor de fotos está intentando abrir un archivo de imagen, pero como se le indica que se trata de un archivo de texto no puede hacerlo y envía ese error.

De esta manera muy sencilla es como se puede observar que se está ocultando un archivo, más no su contenido. Aunque el archivo sea visible como cualquier otro, no se puede acceder a su información. No es porque la información se haya transformado; de hecho, la información no se tocó, simplemente se modificó la extensión del archivo y el sistema operativo no es capaz de abrir el mensaje. De esta manera, queda invisible para aquellos que no conozcan la extensión o el programa con que deben abrirlo.

Actualmente, existen diversos softwares que permiten esconder archivos dentro de otros; por ejemplo, open puff que permite esto mediante una serie de pasos muy sencillos. Hay que agregar un *password* para **desocultar** el archivo que se pretende esconder, incluso existen unos programas que piden dos o tres *password*s para añadir seguridad. Se selecciona el archivo que se desea esconder, que podría ser un archivo de extensión txt ode texto, después se debe de seleccionar el archivo en donde se esconderá el archivo de texto, podría ser un mp3 o de música; de esta manera se podrían ocultar datos confidenciales; por ejemplo, del banco, en un archivo de mp3, y así nadie sospecharía que en una canción que se puede reproducir con el celular, se encuentren datos de acceso delbanco.

Como puedes observar, este subtema está relacionado con el objetivo tercero de la seguridad: confidencialidad de datos. A través de la encriptación u ocultación del contenido del mensaje, o a través de la ocultación del mensaje en sí, se pueden enviar mensajes a través de una red manteniendo la **confidencialidad**. Como se observó, la *esteganografía* es el arte de ocultar un mensaje, y la *encriptación* es el arte de esconder el contenido del mensaje; es decir, mientras en la *esteganografía* esconde el mensaje por completo y no se percibe o no se sabe de la existencia del mensaje, la encriptación permite verlo, pero no así su contenido.

A continuación, se exponen más mecanismos para lograr la seguridad de la información.

3.2. Mecanismos de seguridad

Los mecanismos de seguridad son una serie de recomendaciones que hace la Unión Internacional de Telecomunicaciones ITU (*Internacional Telecommunication Union*) a través de la recomendación x800 (UIT, 2008). Éstas se dividen en dos partes, por un lado,aquellas que se implementan en una capa específica, de acuerdo con el modelo de referencia OSI, y las otras que no son específicas de ninguna capa; se puede decir que estas últimas son mecanismos generales de **seguridad** (Stallings, 2004).

Los mecanismos específicos de seguridad, o mecanismos que se implementan en una capa específica de acuerdo con el modelo de referencia OSI, son (Stallings, 2004):

- Cifrado
- Firma digital
- Control de acceso
- Integridad de los datos
- Intercambio de autentificación
- Relleno del trafico
- Control de enrutamiento
- SSL

Los mecanismos generales son aquellos que no dependen de una capa específica, según el modelo de referencia OSI. De esta manera, los siguientes mecanismos no dependen de alguna de las siete capas del modelo OSI en especial, sino que pueden depender de dos o más de las capas del mismo modelo:

- Funcionalidad fiable
- Etiquetas de seguridad
- Detección de acciones
- Informe para la auditoría de seguridad
- Recuperación de la seguridad

A continuación, se exponen los mecanismos de seguridad que se implementan en las capas del modelo OSI.

Cifrado o **encriptación**: se refiere al uso de algoritmos matemáticos para transformar datos en una forma inteligible, la transformación y su posterior recuperación de los datos depende de un algoritmo (se verá a detalle más adelante). El cifrado lleva a cabo su función en la capa de trasporte del modelo OSI. Lo hace en esta capa ya que siguiente es la de aplicación, que es donde el mensaje debe estar listo para su uso. El **cifrado** o la encriptación es cuando se **modifica** el mensaje original por otro que no pueda ser leído fácilmente. Existe, por ejemplo, un método de encriptación muy común para sitios web que, en programación de páginas, se usa como una función, se llama md5. No

entraremos en detalle con la funcionalidad de este método, pero, si se desea encriptar una palabra, por ejemplo *Hola*, se escribiría así: f688ae26e9cfa3ba6235477831d5122e, existen conversores en Internet de textos planos o sin cifrar a texto cifrado en md5. Como se puede observar, el texto en md5 ya no tiene el mismo sentido que la palabra *Hola;* por ello se dice que el cifrado transforma los datos y, en este caso, el texto a una forma ininteligible.

Firma digital: son datos **añadidos** a los datos o a su transformación cifrada que permiten verificar al usuario la fuente y la integridad (se verá a detalle más adelante). Al igual que el cifrado, la firma digital lleva a cabo sus funciones en la capa de transporte. Podemos pensar en la firma digital como una serie de datos que añaden al mensaje original, de tal manera que deben de corresponder con los que podamos tener almacenados. Es lo mismo que una firma que usamos cotidianamente para expresar nuestro consentimiento a un contrato, sólo que esta firma es totalmente digital.

Control de acceso: es una serie de mecanismos que permiten **dar** o **quitar** derechos de acceso a recursos informáticos. Un ejemplo de esto son los roles o tipos de permisos para administrar ciertas aplicaciones, tales como administración y usuario normal. Estos permisos se dan comúnmente en la capa de aplicación, pues es ahí donde comúnmente se definen los roles de usuario.

El control de acceso son los permisos que se proporcionan a un determinado usuario para hacer o no hacer alguna actividad; por ejemplo, hablemos del portal que utilizas para realizar tus actividades académicas, en él tú tienes permisos de alumno, puedes leer el contenido de las asignaturas, subir tus actividades, etcétera. Tu Facilitador(a) tiene permisos de editar tus calificaciones, de acuerdo con las rúbricas establecidas. Existe, además, un usuario encargado de integrar los contenidos en el sitio donde accedes a ellos para que puedas leerlos como ahora estás leyendo este. El control de acceso permite establecer y definir roles específicos a usuarios específicos.

Integridad de los datos: es un mecanismo diseñado para comprobar la **integridad** de los datos. La integridad de datos es lo opuesto a la corrupción de datos. En algunos casos puede ser verificada mediante algún hash de caracteres, es decir, una cadena de datos.

Cuando se realiza mediante software la comprobación de un hash, se obtiene una cadena de datos que debe ser comparada con la original; esta original suele venir en la página en donde se descargó el recurso. La integridad de los datos se da en casi todas las capas del modelo OSI. Como recordarás, de las capas dos a la siete existe un **control** de errores que permite que se chequen los PDU enviados, con el fin de evitar la corrupción de errores.

Intercambio de autentificación: es un mecanismo diseñado para **comprobar** la **identidad** de algo o alguien, mediante el intercambio de información. Esto es, por ejemplo, un caso avanzado de login; es decir, que además de pedir un sistema un usuario/*password*, podría requerir de algún dato adicional, tal como una pregunta extra, el uso de alguna tecnología

biométrica, etcétera. Esta autentificación se lleva a cabo en la capa de **aplicación**.

El **relleno de tráfico**: se refiere a la **inserción** de bits en espacios en un flujo de envío de datos; por ejemplo, en cada espacio entre dato y dato que se envía en un flujo de datos (algo similar a los espacios que utilizamos en la escritura humana), se adicionan bits, a fin de dificultar su lectura por personas ajenas al mensaje, un modelo que ilustra este mecanismo es cuando se escriben entre cada palabra letras de relleno, de manera tal que el mensaje original no pueda ser leído. Este relleno de tráfico se lleva a cabo en la capa **física**, ya que se envían bits de más a fin de que parezcan datos.

El **control de enrutamiento**: se refiere a **tomar el control** de las rutas por las que deberían pasar los paquetes, recordemos que los **routers** son los dispositivos capaces de *enrutar* la información; es decir, ellos decidirán qué camino debe tomar un paquete de datos de acuerdo con el destino. El control de enrutamiento se refiere a la capacidad de cambiar esa ruta destino, a esto se le conoce en el mundo de las redes como ruteo estático, ya que el usuario puede definir qué rutas debe tomar el paquete y no dejar que el ruteador decida por él. Este tipo de ruteo se lleva a cabo desde la capa 3, red.

Capa de conexión de puerta segura SSL (*Secure Socket Layer*): serie de herramientas criptográficas que permiten comunicaciones seguras, un ejemplo de SSL son las conexiones de red VPN que trabajan con SSL, de manera tal que permiten **encriptar** el envío y la recepción de información. SSL trabaja en dos capas del modelo OSI, una es a nivel de **aplicación,** como por ejemplo el protocolo HTTP, y con la capa de **transporte** (protocolo TCP). Un ejemplo del SSL aplicado es el protocolo HTTPS, que es la implementación segura de HTTP; segura porque usa SSL y, de esta manera, el contenido de HTTP viaja encriptado a través de una red. Los mecanismos generales, es decir, los que no dependen de una capa en específica, se explican a continuación:

Funcionalidad fiable: se refiere a la correcta **aplicación** de **políticas** de **seguridad.** Éstas siempre dependerán de la empresa o de la organización; por ejemplo, puede ser parte de una política de seguridad la aplicación de parches de sistema operativo (en sistemas operativos Windows se les conoce como actualizaciones). Estos parches deberán ser instalados sólo en horarios nocturnos para evitar una interrupción en el servicio (que presta el equipo al que se le aplicarán los parches de seguridad).

Etiquetas de seguridad: son marcas que designan **atributos** a un recurso; podría ser, por ejemplo, que mediante estas etiquetas se puedan distinguir rápidamente equipos cuyo funcionamiento es más crítico (importante) que otros.

Detección de acciones: se refiere a la capacidad de una organización de **monitorear** las acciones de lo que pasa en los sistemas, pero a nivel de red; en estos casos, por ejemplo, es común el uso de equipos que controlan o vigilan lo que sucede en una red, es decir, se coloca un equipo que recoja las bitácoras de ciertas acciones de los demás.

Informe para la auditoría de seguridad: se refiere a la **recopilación** de datos de una revisión y de los exámenes de sistema que se llevan a cabo de manera local. Comúnmente, es como una bitácora de aplicación o de sistema operativo.

Recuperación de seguridad: se refiere a las **peticiones** o mecanismos, automatizados o no, de las acciones que logran recuperar un sistema; por ejemplo, un respaldo de una base de datos.

Como puedes observar, todos estos mecanismos de seguridad permitirán a una organización estar **segura** frente al tráfico de red que circula en torno a una organización, ya que la correcta aplicación de los mecanismos de seguridad, vistos anteriormente, permitirá que toda la información que entre o salga de la organización no esté comprometida con fallas de seguridad. Este aseguramiento permite tener un control de la información que entra y que sale de una organización, y permite saber con certeza a quién se le envió y quién la recibió. Un mecanismo que permite tener certeza de quién envía la información son las firmas y los certificados digitales, tema que se desarrollará a continuación.

3.2.1. Firmas y certificados digitales

Las firmas y los certificados digitales permiten garantizar que el software es genuino, o que una comunicación entre computadoras es genuina; es decir, si por ejemplo visitamos el portal de un banco, debemos revisar con el navegador de Internet que estemos utilizando que su certificado sea válido; de no serlo, estaríamos en el portal de alguien más, pero no de nuestro banco, es decir, podríamos ser víctimas de algún tipo de fraude. Para el caso de una firma, ésta se añade en el mensaje que se envía o en el software quese tiene, a veces es posible revisar esta firma mediante una revisión de algún sitio.

Existen asociaciones encargadas de emitir certificados digitales válidos a las diferentes empresas de Internet (Diccionarios Oxford-Complutense, 2002). Este certificado se almacena en un equipo de cómputo de manera tal que, cada que se ingrese desde este equipo de cómputo a un portal web de una empresa con este certificado, éste validará que sea genuino y, en caso de no serlo, puede enviar una notificación en pantalla. En el ámbito de las redes, ambos casos ayudan en asegurar que la interconectividad que se realiza entre el equipo de cómputo con el certificado y el sitio web al que se accede sea elsitio web que dice ser y, de esta manera se evita caer en fraudes.

La firma digital forma parte de los mecanismos de seguridad revisados en el tema anterior, pero **¿qué es una firma digital y para qué sirve?**

Se conoce como *firma electrónica* a un conjunto de **datos** que se adjuntan a un mensaje electrónico. Permite al receptor de un mensaje **verificar** la autenticidad del emisor de la información, así como verificar que no ha sido modificada desde su generación. Así, la firma electrónica ofrece el soporte para la autenticación e integridad de los datos (BNE, 2012).

Como ejemplo de uso de la firma digital en México se propone las que expide el Servicio de Administración Tributaria SAT para la declaración de impuestos. Con esta herramienta se revisa que la declaración lleve la firma, y garantiza al SAT que el contribuyente está enviando sus datos correspondientes a la declaración de impuestos, así como que los datos que envíe el contribuyente sean verificados, que realmente se trata del contribuyente que los envía, y que los datos no han sido alterados; es decir, que el archivo resultante de una declaración de impuestos no haya sido modificado en el camino,porque puede suceder que el archivo resultante de la declaración de impuestos enviado por correo tradicional sea interceptado, y se cambie la declaración por otra que no corresponde. La firma electrónica, como tal, es la versión electrónica de una **rúbrica** que comúnmente se hace a mano; dicha rúbrica permite conocer que los firmantes están de acuerdo con algo, por ejemplo un contrato. En este caso, la firma electrónica es el medio electrónico que permite identificarse como persona física o moral ante cualquier instancia, ya sea un banco, una aseguradora, etcétera.

Los certificados digitales son documentos electrónicos que proporciona una autoridad de confianza o de certificación. Las partes principales de los certificados digitales son el propietario del certificado o nombre distinguido del sujeto, clave pública, presencia de la institución que lo expide a través de una firma digital y la fecha de validez (CERT, 2012). Un certificado digital sirve también para **identificar** a un titular.

Hasta este punto te preguntarás: ¿Cuál es la diferencia entre un certificado digital y la firma electrónica? Ésta radica en que el certificado electrónico identifica a una persona. El **certificado digital o electrónico** es el equivalente a una **cédula** de identificación, en el caso de México es la credencial de elector. Cuando decimos que es equivalente nos referimos a que no es la cédula de identificación física que tenemos en sí, pero podría ser un archivo de texto encriptado con nuestros datos personales.

La **firma electrónica** es un dato muy parecido a la firma autógrafa. Al igual que ésta, la firma digital sirve para dar fe de que estamos de acuerdo con algo. La firma electrónica depende del certificado digital porque en éste se encuentran las credenciales que identifican a los ciudadanos como entidad o como persona. Es similar a la credencial de elector cuando se requiere realizar un trámite; cuando se solicita empleo, generalmente uno de los requisitos es mostrar la credencial de elector como identificación oficial ante alguna institución; para demostrar que se está de acuerdo con un contrato, en ocasiones solicitan firmar de manera autógrafa algunos documentos y, para que tenga validez esta firma, debe ser exactamente igual o muy parecida a la que se encuentra en la credencial de elector.

Los certificados y las firmas digitales ayudan a dar la **confiabilidad** y la **seguridad** de que una entidad o una persona es quien dice ser. Esta seguridad y confiabilidad radica en la fortaleza que tienen los elementos de identificación electrónicos, que se da por técnicas criptográficas que permiten cifrar la información y, además, ayudan a verificar que el contenido del certificado no haya sido adulterado; por lo cual, se puede intuir que este tipo de identificación electrónico es mucho más confiable que los métodos tradicionales. **¿Y que son las técnicas criptográficas?** Esto se expondrá en el subtema siguiente.

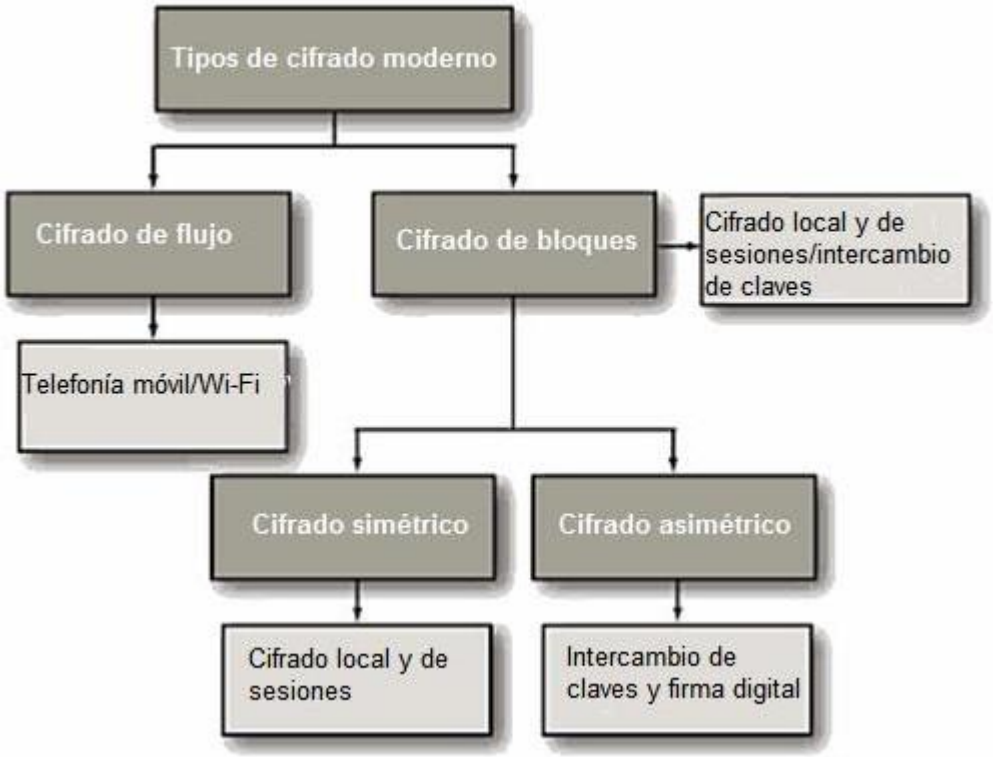
3.2.2. Criptografía

En el subtema 3.2.1. Criptología y esteganografía, se mencionó que la *criptografía* es parte de la *criptología*, que es el estudio de las comunicaciones secretas. Ésta se divide en dos campos de estudio que se complementan entre sí:

- La criptografía: es una técnica que se usa para ocultar la información, es decir, encriptarla (Rajsbaum's, 2005).
- Criptoanálisis: es el estudio que analiza los mecanismos que permiten violar los sistemas de comunicación secretas, o desencriptar la información, sin conocer el *password* o contraseña (Rajsbaum's, 2005).

La raíz etimológica de criptografía proviene del griego *kryptos*, ocultar, y de *grafos*, escribir, que significa escritura oculta. Son las técnicas utilizadas para **cifrar** y **descifrar** información utilizando técnicas matemáticas que hacen posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos(Rajsbaum's, 2005).

Existen dos grandes tipos de cifrado: por bloques y por flujo (Pacheco y Jara, 2012).



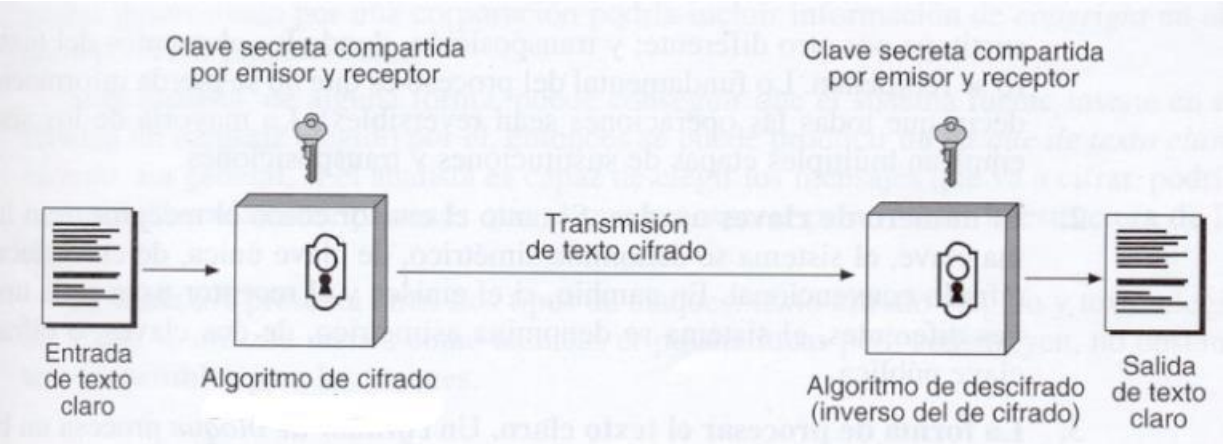
Tipos de cifrado moderno. Fuente: Pacheco y Jara, 2012.

En la imagen anterior se observan los dos grandes tipos de cifrado, se observa que el deflujo es usado por la telefonía móvil o Wi-Fi, que corresponde a la clave de un *access point* de Internet; por ejemplo, en el caso de los Infinitum se sabe que, para acceder a Internet usa una clave o *password*, que es el cifrado de flujo que permite encriptar los datos que se envían y reciben por el *access point*. En el caso del cifrado por bloques, se observan dos tipos de cifrado:

a) Cifrado simétrico o de clave secreta
b) Cifrado asimétrico o de clave pública

El **cifrado simétrico o de clave secreta**, como su nombre lo indica, es aquel que tiene una clave secreta, y una vez que se conoce se podrá **acceder** al mensaje (Rajsbaum's, 2005).

Se le dice que es de cifrado local y de sesiones, ya que este tipo de encriptación es muy usado para, de manera local, compartir archivos que estén encriptados; por ejemplo, existen programas que permiten guardar información de texto en un archivo, y para poder abrirlo se necesita el *password*, tal como sucede con KeePass, que permite generar un archivo en donde podemos guardar muchas contraseñas de diversas índoles, como por ejemplo de acceso a sitios web, de correo electrónico, bancarias, etcétera, y permite recuperar las contraseñas haciendo uso sólo de una contraseña; con la cual, una vez ingresada de manera correcta permite ver el contenido del archivo; es decir, las contraseñas guardadas en el archivo.



Ejemplo de cifrado simétrico Fuente: Rajsbaum's, 2005, p. 4.

En la imagen se puede observar cómo la **Entrada de texto claro** (texto sin encriptar) entra o pasa por un algoritmo de cifrado, que es un conjunto de pasos o instrucciones que cifrará o encriptará el texto; por ejemplo, el algoritmo AES o DES (no entraremos en detalle de lo que hace cada algoritmo, sólo se pretende dar una idea en general de qué es lo que pasa con éstos). La diferencia básica entre AES y DES, es que éste último (Data Encryption Standard o Estándar de Encriptación de Datos) usa una llave de encriptación de 56 bits. La llave de encriptación es el *password* que se usa para desencriptar la información. AES (Advanced Encryption Standard o Estándar de Encriptación Avanzado), por su parte, puede usar llaves de encriptación de 128, 192 o 256 bits. Te preguntarás ¿De qué sirve la llave de encriptación? Pues mientras más grande sea, más difícil es dedescubrir mediante un ataque de fuerza bruta. Un ataque de fuerza bruta es aquel en el que se intenta descubrir un *password*, para ello existen mecanismos en los que a través de diferentes combinaciones de letras y números se pretende adivinar la contraseña. Cuando ésta sea de mayor longitud será más difícil de adivinar.

Una vez cifrado el mensaje se transmite hacia el destino quien, para leer el mensaje, debe conocer la clave secreta o datos de acceso. Una vez que ingresa esta clave en el mensaje cifrado, podrá ser leído. Para que quede esto más claro, considérese el siguiente ejemplo.

Se utilizará un sistema que se denomina sustitución mono alfabética, que se expone a continuación:

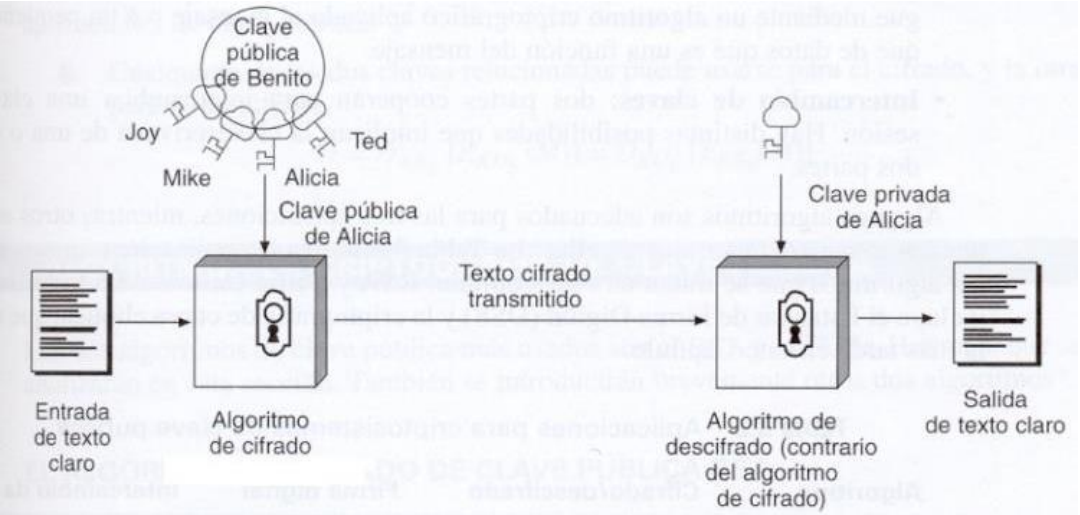
Texto simple: ABCDEFGHIJKLMNÑOPQRSTUVWXYZ Texto cifrado: QWERTYUIOPASDFGHJKLÑZXCVBNM

Si se desea cifrar el texto HOLA, se obtendría el texto cifrado IHSQ, ¿Cómo se realiza el procedimiento?, se explica a continuación:

La H es la letra 8 del alfabeto, entonces se toma la letra 8 del texto cifrado: I
La O es la letra 16 del alfabeto, entonces se toma la letra 16 del texto cifrado: HLa L es la letra 12 del alfabeto, entonces se toma la letra 12 del texto cifrado: S La A es la letra 1 del alfabeto, entonces se toma la letra 1 del texto cifrado: Q

En el caso de este cifrado simétrico, es muy importante que tanto emisor como receptor **conozcan** la clave. Esto supone un problema, ya que podría ser necesario hacer que se reúnan o se llamen vía telefónica emisor y receptor. Para resolver este problema, se usa el cifrado asimétrico.

El **cifrado asimétrico o de clave pública** es aquel en el que no se usa una sola clave para encriptar o desencriptar (cifrar o descifrar), sino que se usan más. Tiene la característica de que usa una para cifrar y otra para descifrar; en este caso, comúnmentela clave de cifrado es pública y la de descifrado es privada. La clave de cifrado se dice que es pública porque es la que se debe de **compartir** con quienes se desee o se requiera compartir información. La clave privada es aquella que sólo el receptor conoce.



Ejemplo de cifrado asimétrico. Fuente: Rajsbaum's, 2005, p. 27.

En este esquema se puede apreciar que el texto claro o sin cifrar entra al algoritmo de cifrado, se **encripta** con la clave pública de Benito y envía el texto cifrado a Alicia, quien toma el mensaje y lo **desencripta** con su clave privada. Una vez que lo hace podrá ver el mensaje que le envió Benito. Para que esto sea posible existe un concepto llamado **llavero**. En el llavero de Benito, que es público, se encuentra la clave privada de Alicia, de manera cifrada, y como se puede ver en el esquema, cuenta con más llaves, pero como el mensaje es de Benito para Alicia, el cifrado se hace exclusivo para la llave de Alicia, por lo que Alicia es la única que puede abrir y leer el mensaje. La desventaja de este tipo de cifrado es que utiliza más poder de cómputo, es decir, recursos de memoria RAM y CPU que el cifrado simétrico, esto por lo complejo que se vuelve un mensaje encriptado. La complejidad radica en su algoritmo RSA, que es de los más seguros hasta el momento, pero que, por cuestiones de enfocarnos al tema de criptografía, no tocaremos; sólo se explicará brevemente en qué consiste. La seguridad del algoritmo RSA (llamado así en honor a sus diseñadores: Rivest, Shamir y Adleman) radica en la dificultad de la factorización de números grandes, del orden de 100 dígitos. Recuerda que un número primo es aquel que sólo es divisible entre uno y él mismo. *Factorizarlo* es descomponerlo en los números que multiplicados entre sí nos den como resultado el original (Moliner, 2005).

El concepto de **llavero** es un archivo que sirve como almacén de llaves públicas de las personas con las cuales queremos intercambiar mensajes (Rohaut, 2012).

Existen algunas instrucciones que ayudan a la hora de programar para usar los métodos aquí descritos, todo dependerá del lenguaje de programación que se esté usando; así, por ejemplo, en el lenguaje de programación PHP (en la asignatura Programación Web I se explicará a detalle en qué consiste), existen las “extensiones criptográficas”, con las cuales se pueden encriptar y desencriptar mensajes y hacer verificaciones de certificados digitales.

Como se puede observar, cada tipo de cifrado de los que se revisaron tiene sus ventajas y sus desventajas. Así pues, la ventaja del cifrado simétrico consiste en que es sencillo de descifrar, por lo que usa muy poco poder de cómputo, pero no muy seguro en comparación con el cifrado asimétrico, que es muy seguro, pero gasta mucho poder de cómputo. Es importante que consideres las formas de cifrado para que, como futuro ingeniero de software, puedas decidir qué tipo de encriptación se puede adecuar a tus desarrollos, aunque también es importante mencionar que, dependiendo del mensaje, datos o información a enviar, puedes **evaluar** qué tipo de encriptación utilizar; dependerá de qué tanto te conviene mantener oculto un mensaje. Podría suceder que envíes un mensaje cuyo contenido tiene relevancia para un periodo determinado de tiempo, por ejemplo: una invitación a algún evento cuyo mensaje una hora después de enviarlo ya no sea relevante. Para ello se podrían utilizar cifrados simples que, si bien se pueden rompero deducir con cierta facilidad, para cuando un intruso descifre el mensaje éste ya no será relevante.

El tipo de encriptación a utilizar dependerá de la **relevancia** y la importancia del mensaje, por ejemplo, mientras más relevancia e importancia tenga, más fuerte deberá ser el nivel de encriptación, ahora la pregunta es ¿Cómo saber si un mensaje es o no relevante e importante? Esto es, entre otras cosas, el campo de estudio de algo que se le denomina políticas de seguridad y que se revisará a continuación.

3.2.3. Políticas de seguridad

Las políticas de seguridad son normas y procedimientos que crea y que rige a una organización. Las políticas de seguridad de una empresa siempre serán diferentes a las de otras, esto dada la heterogeneidad de cada organización; en otras palabras, cada empresa tendrá diferentes sistemas informáticos, diferentes protocolos de uso, diferente interconectividad de sus equipos a la red, diferentes administradores de sistemas, diferentes sistemas operativos en sus equipos de red y en sus equipos de cómputo, por ello las políticas de seguridad siempre serán propias de cada empresa. Aquí revisaremos un concepto, en general, que nos dará una idea de cómo se hacen estas políticas y para qué sirven.

Tú como desarrollador de software deberás también saber cómo se hacen y se tratan las políticas de seguridad, ya que seguramente algún desarrollo que te soliciten en el ámbito laboral deberá cumplir con alguna normativa; por ejemplo, el uso de encriptación de *password* bajo algún método; otra normativa podrá ser que el código cumpla con ciertos estándares que pueden o no ser parte de alguna ISO, simplemente puede ser el estándar que usa en una organización, por ejemplo, el uso de notas y comentarios en el software que vas desarrollando.

Las políticas de seguridad recogen las directrices u objetivos de una organización con respecto a la seguridad de la información, estas forman parten de su política general y deben ser aprobadas por la dirección. Por ello, las políticas de seguridad pueden ser diferentes entre diversas organizaciones, o pueden poner más énfasis en unas políticas o en otras, aunque también existen algunos estándares de seguridad para países o para áreas (gobierno, medicina, militar, etcétera). Algunos más internacionales son definidos por la ISO (Aguilera, 2010).

Una política de seguridad, según Aguilera (2010), contendrá todos los elementos en materia de seguridad de la información, generalmente englobados en cinco grupos:

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos sobre un eventual ataque.

- Relacionar todas las medidas de seguridad que deben de implementarse para afrontar los riesgos de cada activo o grupo de activos.

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en cada uno de los departamentos de la organización.

- Detectar todas las vulnerabilidades del sistema de información y controlar fallos que se producen en los activos, incluidas las aplicaciones instaladas.

- Definir un plan de contingencias.

Para detectar vulnerabilidades en los sistemas de información es necesario llevar a cabo auditorías de sistemas, por ellas se entiende un análisis a detalle de un sistema que permita conocer, descubrir, identificar y corregir vulnerabilidades en el o los sistemas deinformación. Un análisis de vulnerabilidades deberá tener, según Aguilera (2010), como mínimo:

- Descripción y características de los activos (equipo de cómputo o de red) y los procesos analizados

- Análisis de las relaciones y dependencias entre activos y procesos de información

- Relación y evaluación de las vulnerabilidades detectadas en cada activo y proceso de información

- Verificación del cumplimiento de la normatividad de la seguridad de la información

- Propuesta de medidas preventivas o correctivas

Para llevar a cabo la auditoría es necesario que se cuente con algunas herramientas para el **análisis**, tales como manuales de los activos y software para auditorías. Por ejemplo, para el caso de las redes inalámbricas, se puede hacer uso de herramientas como Wi-Fi Slax, el cual nos ayuda a probar las vulnerabilidades de las redes.

En caso de que sea vulnerada la seguridad de la organización, y de hecho, antes de que suceda, es muy importante que se cuente con un plan de contingencias, en cual se plasme qué hacer, de esta manera la organización será capaz de responder y de continuar con sus operaciones habituales. Un plan de **contingencias** para que sea exitoso, deberá estar focalizado en los siguientes tres ejes, según Aguilera (2010):

- **Plan de respaldo**: medida preventiva en la cual se pide se hagan respaldos periódicos de la información y de la configuración de los equipos, sean de cómputo o de red, y que deberá ser conservada en lugares seguros.

- **Plan de emergencia**: contempla qué medidas se deben de tomar cuando se esté llevando a cabo una amenaza; por ejemplo, en el caso de un ataque de denegación de servicio (DoS, *Denial of Service*,), cerrar los puertos por los que se está llevando a cabo un ataque o bien apagar el equipo. Un ataque de DoS, es aquel en el que se emiten muchas

peticiones a un servidor, por ejemplo, se puede llenar un servidor web de peticiones a fin de hacer que el equipo sea incapaz de responder las peticiones.

- **Plan de recuperación**: tiene que ver con las medidas que se van a aplicar después de un desastre, con ello se evalúa el daño y se hace lo posible para regresar a la operación normal el equipo que fue atacado.

Hasta este punto te preguntarás, ¿y cómo puedo hacer una red segura? Pues bien, lo primero es saber cuáles son los elementos que conforman a la red que se pretende asegurar, es decir, considerar los siguientes planteamientos:

- **¿Con qué dispositivos de red se cuenta**? Es importante conocer qué dispositivos de red hay para saber cómo se conforma de manera **topológica**. Conocer la topología de la red permite saber la manera en la que se **conectan** físicamente todos los equipos. Así se podría **evaluar** si la distribución física de la red es óptima o si se propone otra forma, así como también saber en qué lugares se pueden **colocar** equipos de seguridad de la red.

- **¿Con qué tipos de servidores se cuenta y cuáles son sus sistemas operativos?** Saber qué servidores se tienen en la organización permitirá, por un lado, conocer los servicios que se brindan en esa organización mediante los servidores, y saber su sistema operativo permitirá **definir** una política de seguridad adecuada al equipo que se trate; por ejemplo, para el caso de contar con equipos con cierto sistema operativo,se deberá **crear** un dominio en la red de manera tal que se encargue de administrar las actualizaciones de seguridad. Cuando se están conociendo los servidores de la organización es muy importante saber qué puertos usan para **brindar** los **servicios** para los cuales están destinados; por ejemplo, para un servidor de páginas web, el puerto que comúnmente está asociado a este servicio es el 80, si se tratase de un servidor de base de datos MySql, el puerto por default que está asociado a éste es el 3306. Se puede buscar la información de puertos asociados a cada servicio en Internet, aunque es importante mencionar que a veces estos puertos pueden ser fijados por la persona que instala el servicio en un servidor; de esta manera, se podría tener un servidor de páginas web que no use el puerto 80 sino el 90, este cambio no obedece a nada más que a una modificación en la configuración original de la instalación de un servicio.

- **Revisar si la red de la organización está segmentada** (es decir, que existan subredes) y si está segmentada saber ¿Cuántos segmentos la conforman? Saber si en la organización existe más de un segmento permite tener una visión más general de toda la red, y de esta manera conocer sus **dimensiones** reales. También permite conocer las **causas** por las que la red está segmentada. Podría tratarse de una segmentación por tipo de departamento, o por importancia de equipo de cómputo, por ejemplo: servidores y usuarios.

- Es necesario **investigar si existe algún tipo de infraestructura de red que permita asegurar la red.** Saber si existe una infraestructura de red que permita **asegurarla**, se refiere a saber si en la red existen dispositivos como un **firewall.** Esto permitirá conocer el nivel de seguridad actual. Es importante que si existe uno o más firewalls en la organización se deban conocer las políticas establecidas dentro de éstos. Las políticas de firewall son el conjunto de limitaciones o permisos que tiene configurados el equipo, con base en ellas se definen qué servicios pueden entrar o salir de la organización a Internet (Andreu, 2010). Recuerda que cuando se mencionan servicios son, por ejemplo, servicio web, servicio de correo electrónico, etcétera.

Identificar cuáles son los equipos más importantes para la organización. Esto permite identificar los equipos más sensibles para la organización, es decir, qué servidores son los más **importantes** y de los cuales la organización no puede prescindir. Así se les dará mayor importancia.

Considerar si existen políticas de seguridad. Esto permitirá conocer las medidas que se han tomado en la organización para hacer **frente** a las **amenazas** de su red y de sus **aplicaciones**, así como evaluar o reevaluar las políticas de seguridad. Recuerda que éstas deben, a grandes rasgos, considerar los siguientes aspectos:

- Identificar los riesgos
- Detectar vulnerabilidades en los sistemas y mitigarlos
- Evaluar el impacto en caso de un ataque
- Definir un plan de contingencias

Por identificar los riesgos, entiéndase buscar y tener en cuenta todos los riesgos de los sistemas; es decir, localizar los equipos que, de fallar, tendrían un **impacto** grande en la organización; por ejemplo, que se descomponga el servidor de correo electrónico, que se descomponga el servidor de páginas web, que la organización se quede sin Internet, etcétera. Por detectar las vulnerabilidades entiéndase, por ejemplo, sistemas que se han dejado con la configuración por default, *passwords* que son sencillos de adivinar. La configuración por default de un programa es un problema de vulnerabilidad por lo siguiente: muchos utilizan la instalación estándar y ya no configuran o personalizan a su gusto, por ello se tiene configuraciones iguales en muchos dispositivos. Lo más peligroso de estas configuraciones es tener la misma combinación de usuario *password*, y se hace más peligrosa, cuando al usuario tiene privilegios administrativos.

Por evaluar el impacto, en caso de un ataque, se entiende la necesidad de tener una visión a futuro y definir qué pasaría en el mejor y en el peor de los escenarios. Por ejemplo, si atacan un servidor de correo electrónico, en el mejor de los casos se deja sin servicio por un rato, y en el peor de los mismos se perdería el servidor de correo por completo con todo su historial.

Una vez definidos los impactos ante algún ataque es necesario establecer un plan de contingencias que permita recuperarse después de un ataque lo antes posible. Un plan de contingencias permite que se actúe en forma más cautelosa en relación con la tecnología de información, equipo de cómputo, equipo de red, etcétera; y de esa manera reaccionar cuanto antes a un ataque y evitar desastres. ¿Te imaginas perder toda la información de tu disco duro? El tener un plan de contingencias permite que no pierdas tu información o la menor información posible.

Como se ha podido observar, la seguridad en los sistemas de la información juega un papel muy importante en cualquier organización a cualquier nivel, ya que están en peligro datos o información que es muy importante para la empresa o el negocio. La seguridad en los sistemas de la información abarca las aplicaciones y desarrollos; mientras que la seguridad en las redes se refiere a la seguridad en los sistemas de información en cuanto a networking. Es importante mencionar que como desarrollador de software puedes apoyar en la identificación o propuesta de integración de herramientas que apoyen en la protección de las amenazas o los ataques a los desarrollos, la mejor manera es apegándote a las normas o políticas de seguridad o políticas de seguridad en redes y en los sistemas de información de la empresa u organización en la que te encuentres laborando, además, es necesario que evites utilizar combinaciones de usuario/password que te dan por default los sistemas o sitios, o utilizar los que son sencillos de adivinar por ejemplo: admin/admin, o admin/123, fechas de nacimiento, de cumpleaños, nombres de personas cercanas, etcétera, es decir, datos que pueden ser obvios. Para tener *password*s más seguros intenta usar combinaciones de números, letras mayúsculas, minúsculas y caracteres especiales, de esta manera tu *password* será más seguro, ya que es más difícil de rastrear.

Cierre de la unidad

En esta unidad se revisó, a grandes rasgos, una visión general de seguridad de la información. En este papel las redes juegan un rol muy importante desde cómo se configura una red, hasta qué accesos se están proporcionando a los usuarios. Se puede intuir, a lo largo de esta unidad, que el usuario juega un papel muy importante para la seguridad. Es aquí donde aplican las políticas de seguridad. Las redes y los sistemas de información por sí solos siempre tendrán huecos de seguridad, pero es tarea de los administradores de los sistemas de información arreglarlos o mitigarlos. Como futuro ingeniero de software también tendrás tus responsabilidades para evitar que los sistemas de información no presenten fallas, y si las hay saber que existen mecanismos que pueden ser implementados.

La interconectividad de redes es algo que se utiliza todos los días, y un ejemplo de ello es tu carrera que está cursando en línea, desde una computadora con acceso a Internet para acceder a tus asignaturas, hasta el servidor en donde se encuentran hospedado todos y cada uno de los contenidos que revisas a diario. Aquí también la seguridad de la información juega un papel importante, ya que la plataforma debe ser capaz de albergar a todos los estudiantes que se conectan a diario para leer, consultar o para entregar sus tareas, y esta plataforma también obedece a ciertas políticas de seguridad a fin de que todos los estudiantes puedan acceder a sus asignaturas y que los datos importantes como calificaciones, mensajes, etcétera puedan estar seguros.

Para saber más

Para saber más acerca de cómo implementar una red segura y su importancia se recomienda consultar los siguientes artículos:

- Search Data Center (2013). *Cómo planificar una red segura mediante la práctica de ladefensa en profundidad*.

- García, R. A. G., & Enr, S. C. (2005). Seguridad en Internet: un estado del arte. Journal of Basic Sciences. https://n9.cl/sccov

Para saber cómo desarrollar e implementar una red segura puedes consultar los siguientes documentos:

- Ardita, J.C., (2001) *¿Cómo desarrollar una arquitectura de red segura?* Buenos Aires: CYBSEC S.A. Security Systems Worktec. [En línea] https://docplayer.es/24839391-Como-desarrollar-una-arquitectura-de-red-segura.html

- Ibarra Ruíz, C. D., Herrera Vásquez, L. A., & Paredes Reyes, M. J. (2019). Análisis de la viabilidad de un estándar de seguridad que implemente técnicas de esteganografía y criptografía para aumentar la seguridad de la información en las empresas. https://n9.cl/owyxo

Para reforzar la importancia de la seguridad en las redes, consulta algunas razones por las que una red inalámbrica debe estar asegurada en el documento:

- Cisco. (2013a). *Aunque no pueda ver su red inalámbrica, protegerla debería ser una de sus principales* prioridades. http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

Puedes consultar algunos consejos de implementación de una red segura en el siguiente documento:

- Lorenzana, D. (2012). *Consejos para implementar una segura red informática en nuestra empresa*. http://www.pymesyautonomos.com/consejos-practicos/consejos-para-implementar- una-segura-red-informatica-en-nuestra-empresa

Fuentes de consulta

Fuentes Básicas

- Aguilera, P. (2010). *Seguridad informática*. Madrid: Editex.
- Andreu, J. (2010). *Servicios en red*. Madrid: Editex.
- Ardita, J.C., (2001) *¿Cómo desarrollar una arquitectura de red segura?* Buenos Aires: CYBSEC S.A. Security Systems Worktec. [En línea] https://es.scribd.com/presentation/350725829/Como-Desarrollar-Una-Arq-de-Red-Segura-Ardita
- Areitio, J., (2008). *Seguridad de la información: redes, informáticas y sistemas de información.* Madrid: Paraninfo.
- BNE. (2012) *¿Qué son la firma y los certificados electrónicos?*
- Cert Superior. (2012). *Certificados Digitales*. https://www.certsuperior.com/
- Cisco. (2013a). *Aunque no pueda ver su red inalámbrica, protegerla debería ser una de sus principales* prioridades. http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html
- Cisco. (2013b). *Tecnología inalámbrica. Protección de las redes inalámbricas*. http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html
- Diccionarios Oxford-Complutense. (2002). *Diccionario de internet*. Madrid: Complutense.
- García, A. y Alegre, M. (2011). *Seguridad informática*. Madrid: Paraninfo.
- Lorenzana, D. (2012). *Consejos para implementar una segura red informática en nuestra empresa*. http://www.pymesyautonomos.com/consejos-practicos/consejos-para-implementar- una-segura-red-informatica-en-nuestra-empresa
- MMC. (2003). *Esteganografía*.

- Moliner, F. (2005). *Grupos A y B de informática. Bloque específico.* Valencia: MAD.

- Pacheco, F. y Jara, H. (2012). *Users: Ethical Hacking 2.0*. Buenos Aires: Dalaga.

- Rajsbaum's, S. (2005). *Criptografía*. http://www.matem.unam.mx/~rajsbaum/cursos/web/presentacion_seguridad_1.pdf

- Ramos, B. y Ribagorda, A. (2004). *Avances en criptología y seguridad de la información.* Madrid: Díaz de Santos.

- Rohaut, S. (2012). *Preparación para la certificación LPIC-1*. Barcelona: ENI.

- Search Data Center. (2013). *Cómo planificar una red segura mediante la práctica de la defensa en profundidad*.

- Sedgewick, R. (1992). *Algoritmos en C++.* Delaware: Addison-Wesley/Díaz de santos. ISBN 0-201-62574-1

- Stallings, W. (2004). *Fundamentos de seguridad en redes: Aplicaciones y estándares*, 2ª ed. Madrid: Pearson Educación.

- UIT. (2008). *X.800 Layer Two Security Service and Mechanisms for LANs*. https://www.itu.int/rec/T-REC-X.800-199610-I!Amd1

- Valencia, L., Guarda, T., Arias, G. P. L., & Quiña, G. N. (2019). Seguridad de la Información en WSN aplicada a Redes de Medición Inteligentes basado en técnicas de criptografía. Revista Ibérica de Sistemas e Tecnologías de Información, (E17). https://search.proquest.com/openview/5720c78f2e17a2735a48f2ca5015a08f/1?pq-origsite=gscholar&cbl=1006393

- Despujol Zabala Ignacio, UPV (2017, 29 septiembre). Medidas de seguridad informática. Encriptado [video]. YouTube. https://n9.cl/64h1p

Fuentes de imágenes:

- Pacheco, F., y Jara, H., (2012). *Users: Ethical Hacking 2.0*. Buenos Aires: Ed. Dalaga, S.A. ISBN 978-987-1857-63-0

- Rajsbaum's, S., (2005). Instituto de Matemáticas, Universidad Nacional Autónoma de Mexico (UNAM).

http://www.matem.unam.mx/~rajsbaum/cursos/web/presentacion_seguridad_1.pdf

- S Secur-IT @C.R.S (2011a). *Información previa a System Hacking.* http://securitcrs.files.wordpress.com/2011/10/system-hacking.png

- Secur-IT @C.R.S (2011b). *Ataques online pasivos System Hackyng*. http://securitcrs.files.wordpress.com/2011/10/man-in-the-middle1.png

- Stallings, W., (2003). *Fundamentos de seguridad en redes. Aplicaciones y estándares*. Madrid: Pearson Prentice Hall.