Seguridad informática

Purificación Aguilera López

EDITEX

1 Introducción a la seguridad informática

vamos a conocer...

1. Sistemas de información y sistemas informáticos
2. Seguridad
3. Análisis de riesgos
4. Control de riesgos
5. Herramientas de análisis y gestión de riesgos

PRÁCTICA **PROFESIONAL**
Estudio de la seguridad en una empresa

MUNDO **LABORAL**
Las personas son el eslabón débil en la ciberseguridad

y al finalizar esta unidad...

- Distinguirás entre sistema de información y sistema informático.
- Comprenderás qué significa seguridad en el amplio concepto de sistema de información y en el concreto de sistema informático.
- Conocerás cuáles son las propiedades de un sistema seguro.
- Podrás entender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto.
- Entenderás lo que son servicios, mecanismos y herramientas de seguridad.
- Tendrás la base necesaria para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos.

CASO **PRÁCTICO** INICIAL

situación de partida

Una clínica dental se dirige a una empresa de servicios informáticos solicitando un estudio de sus equipos e instalaciones para determinar el grado de seguridad informática y los ajustes que se consideren necesarios.

Un trabajador de la empresa informática se dirige a la clínica y mantiene una entrevista con el titular de la misma, quien le informa de los siguientes aspectos:

El personal de la clínica está formado por: el titular, médico especialista en odontología. Como contratados: otro odontólogo, dos auxiliares de clínica y un auxiliar administrativo, que también ejerce como recepcionista, y una persona para la limpieza.

La clínica cuenta con dos consultas, cada una de ellas con un especialista en odontología. En cada consulta hay un ordenador desde el que pueden consultar la base de datos de pacientes tanto el especialista como el auxiliar de clínica que trabaja en esa consulta. En recepción hay otro ordenador con un programa de tipo agenda para consultar las horas libres y anotar las citas. En un despacho aparte están los archivos en soporte papel y donde se encuentra el servidor.

Todos los ordenadores tienen sistema operativo Windows, excepto el servidor que es Linux.

El objetivo de la clínica es proteger la información, especialmente la relativa a los historiales médicos de sus pacientes.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Elabora un listado de los activos de la clínica.
- ¿Cuáles son los activos?

2. Observa qué sistemas de seguridad física y lógica están protegiendo actualmente el sistema. Si están revisados y actualizados.
- ¿Qué es seguridad física y lógica?

3. Comprueba cuáles son las vulnerabilidades del sistema informático, tanto en el software, como en el hardware, el personal y las instalaciones.
- ¿Qué propiedades debe tener el sistema de información para ser seguro?
- ¿Qué amenazas y riesgos existen?
- ¿Qué vulnerabilidades tiene el sistema?

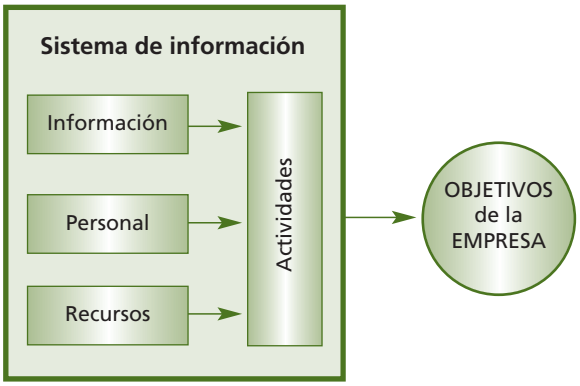
4. Elabora una lista de servicios y mecanismos que incrementarían la seguridad de la información.
- ¿Qué servicios de seguridad se necesitan y qué mecanismos son necesarios para asegurar esos servicios?

5. Investiga si la clínica dispone de una política de seguridad o de un plan de contingencias.
- ¿Está informado todo el personal de la política de seguridad?
- ¿Se realizan ensayos y simulacros según el plan de contingencias?

6. Determina si la clínica requiere una auditoría informática.
- ¿En qué consistirá la auditoría?
- ¿Se realizará con algún software específico para auditoría informática?

1. Sistemas de información y sistemas informáticos

Un **sistema de información** (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus **objetivos.**

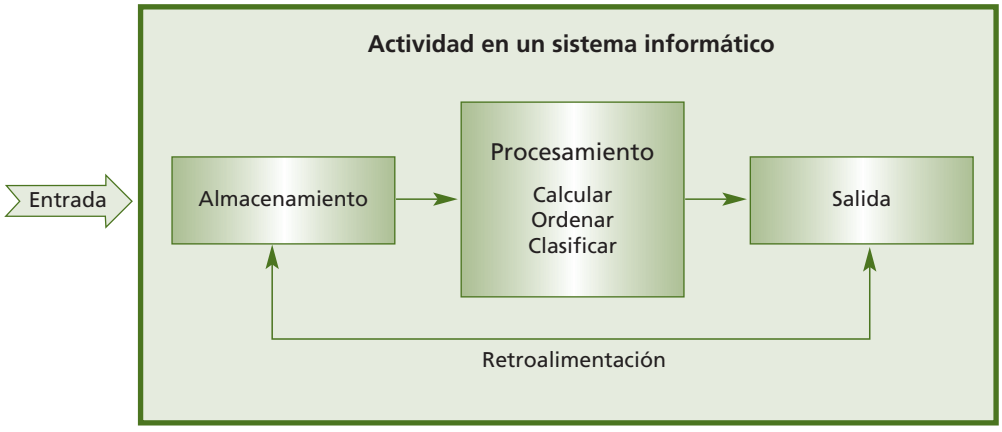


Estos elementos son:

- **Recursos.** Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.
- **Equipo humano.** Compuesto por las personas que trabajan para la organización.
- **Información.** Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.
- **Actividades** que se realizan en la organización, relacionadas o no con la informática.

Sistemas informáticos

Un **sistema informático** está constituido por un conjunto de elementos **físicos** (hardware, dispositivos, periféricos y conexiones), **lógicos** (sistemas operativos, aplicaciones, protocolos…) y con frecuencia se incluye n también los elementos **humanos** (personal experto que maneja el software y el hardware).



Un sistema informático puede ser un subconjunto del sistema de información, pero en principio un sistema de información no tiene por qué contener elementos informáticos, aunque en la actualidad es difícil imaginar c ualquier actividad humana en la que no se utilice la informática. A lo largo de este libro estudiaremos la seguridad en los sistemas de información, en general, y en los sistemas informáticos, en particular, como parte de aquellos.

2. Seguridad

2.1. Aproximación al concepto de seguridad en sistemas de información

Una de las acepciones de la RAE para el término seguro, que es la que aquí nos interesa, es la de estar **libre y exento de todo peligro, daño o riesgo.** Este es el concepto en el que se basa el contenido de este libro y tiene el mismo sentido aplicado a sistemas de información y sistemas informáticos.

La **seguridad informática** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

↑ Sistema seguro.

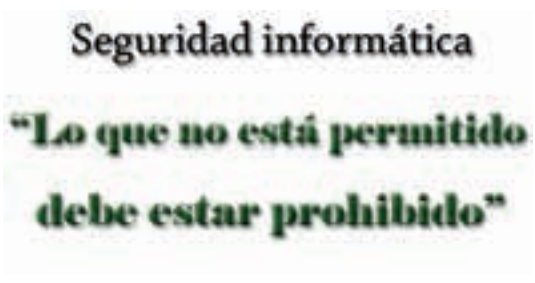
Un sistema de información, no obstante las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

- Cuáles son los **elementos** que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
- Cuáles son los **peligros** que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.
- Cuáles son las **medidas** que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico, revisando y actualizando las medidas adoptadas.

Todos los elementos que participan en un sistema de información pueden verse afectados por fallos de seguridad, si bien se suele considerar la información como el factor más vulnerable. El hardware y otros elementos físicos se pueden volver a comprar o restaurar, el software puede ser reinstalado, pero la información dañada no siempre es recuperable, lo que puede ocasionar daños de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es que la mayoría de los fallos de seguridad se deben al factor humano.



2.2. Tipos de seguridad

Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es ev itar o reducir los riesgos que amenazan al sistema.

Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

Pasiva

Está formada por las medidas que se implantan para, una vez pro ducido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos.

2.3. Propiedades de un sistema de información seguro

Los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización.

Su **origen** puede ser:

- **Fortuito.** Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistema, catástrofes naturales…
- **Fraudulento.** Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, r obo o accidentes provocados.

caso **práctico** inicial

Integridad, confidencialidad y disponibilidad de los datos son las propiedades que debería tener un sistema considerado seguro.

Se considera seguro un sistema que cumple con las propiedades d e **integridad, confidencialidad** y **disponibilidad** de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad que se estudiarán más adelante.

Integridad

Este principio garantiza la autenticidad y precisión de la info rmación sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.

Para evitar este tipo de riesgos se debe dotar al sistema de me canismos que prevengan y detecten cuándo se pro duce un fallo de integridad y qu e puedan tratar y resolver los errores que se han descubierto.

Confidencialidad

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como «el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada».

Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder , a qué parte del sistema, en qué m omento y para realizar qué tipo de operaciones.

Disponibilidad

La información ha de estar disponible para los usuarios autorizados cuando la necesiten.

El programa MAGERIT define la disponibilidad como «grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información».

Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido.

saber más

MAGERIT

Es una metodología de análisis y gestión de riesgos de los sistemas de información. En inglés *Methodology for Information Systems Risk Analysis and Management.*

ACTIVIDADES

1. La biblioteca pública de una ciudad tiene mobiliario, libros, revistas, microfilms, varios ordenadores para los usuarios en donde pueden consultar libros electrónicos, y un ordenador en el que la bibliotecaria consulta títulos, códigos, referencias y ubicación del material bibliográfico.

Indica a continuación de cada elemento con un **sí**, si forma parte del sistema informático de la biblioteca y con un **no** si no forma parte de él:

a) Libros y revistas colocados en las estanterías.

b) Mobiliario.

c) Microfilms.

d) Libros electrónicos.

e) Ordenadores de los usuarios.

f) Ordenador de la bibliotecaria.

g) Datos almacenados en el ordenador de la bibliotecaria.

h) Bibliotecaria.

2. De los elementos relacionados en la pregunta anterior, ¿cuáles pertenecen al sistema de información de la biblioteca?

3. Un incendio fortuito destruye completamente todos los recursos de la biblioteca. ¿En qué grado crees que se verían comprometidas la integridad, la confidencialidad y la disponibilidad de la información?

4. El informático que trabaja para la biblioteca, ¿forma parte del sistema informático de la misma?

5. El ordenador de la biblioteca tiene un antivirus instalado, ¿esto lo hace invulnerable?

6. ¿A qué se deben la mayoría de los fallos de seguridad? Razona tu respuesta.

7. ¿Podrías leer un mensaje encriptado que no va dirigido a ti? Busca en internet algunos programas que encriptan mensajes.

8. ¿La copia de seguridad es una medida de seguridad pasiva?

9. ¿Qué propiedades debe cumplir un sistema seguro?

10. ¿Qué garantiza la integridad?

3. Análisis de riesgos

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema.

«La cadena siempre se rompe por el eslabón más débil».

La persona o el equipo encargado de la seguridad deberá analizar con esmero cada uno de los elementos. A veces el descuido de un elemento considerado débil ha producido importantes fallos de seguridad. Al estar interrelacionados todos los elementos este descuido puede producir errores en cadena con efectos insospechados sobre la organización.

3.1. Elementos de estudio

Para comenzar a analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta los siguientes elementos: activos, amenazas, riesgos, vulnerabilidades, ataques e impactos.

Activos

caso **práctico** inicial

Los activos de un sistema de información: datos, software, hardware y sus accesorios, redes, soportes, instalaciones, personal y servicios.

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos. Al hacer un estudio de los activos existentes hay que tener en cuenta la relación queguardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido a otro.

Podemos clasificarlos en los siguientes tipos:

- **Datos.** Constituyen el núcleo de toda organización, hasta tal punto quese tiende a considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo. El funcionamiento de una empresa u organización depende de sus datos, que pueden ser de todo tipo: económicos, fiscales, de recursos humanos, clientes o proveedores…

  Cada tipo de dato merece un estudio independiente de riesgo por la repercusión que su deterioro o pérdida pueda causar, como por ejemplo los relativos a la intimidad y honor de las personas u otros de índole confidencial.

- **Software.** Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

- **Hardware.** Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información. Incluimos en este grupo los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vía de transmisión de los datos (módem, router, instalación eléctrica o sistemas de alimentación ininterrumpida, destructores de soportes informáticos…).

- **Redes.** Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancia.

- **Soportes.** Los lugares en donde la información queda registrada y almacenada durante largos períodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).

- **Instalaciones.** Son los lugares que albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales o edificios, pero también pueden ser vehículos y otros medios de desplazamiento.

- **Personal.** El conjunto de personas que interactúan con el sistema de información: administradores, programadores, usuarios internos y externos y resto de personal de la empresa. Los estudios calculan que se producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología.

- **Servicios** que se ofrecen a clientes o usuarios: productos, servicios, sitios web, foros, correo electrónico y otros servicios de comunicaciones, información, seguridad, etc.

Amenazas

caso **práctico** inicial

Identificar las amenazas y las vulnerabilidades del sistema permitirá conocer los riesgos potenciales que amenazan la seguridad de un sistema.

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que –de tener la oportunidad– atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

En función del tipo de alteración, daño o intervención que **podrían producir sobre la información,** las amenazas se clasifican en cuatro grupos:

- **De interrupción.** El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

- **De interceptación.** Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

- **De modificación.** Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.

- **De fabricación.** Agregarían información falsa en el conjunto de información del sistema.

Según su **origen** las amenazas se clasifican en:

- **Accidentales.** Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.
- **Intencionadas.** Son debidas siempre a la acción humana, como la introducción de software malicioso –malware– (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática (con frecuencia se produce previa la introducción de malware en los equipos), robos o hurtos. Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma.

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una **amenaza** aprovechando una **vulnerabilidad.** No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (por ejemplo, contratando un seguro).

Vulnerabilidades

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los *hackers*, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Ataques

Se dice que se ha producido un ataque **accidental** o **deliberado** contra el sistema cuando se ha materializado una amenaza.

En función del impacto causado a los activos atacados, los ataques se clasifican en:

- **Activos.** Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.
- **Pasivos.** Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento «víctima» directamente, o a través de recursos o personas intermediarias.

saber más

Algunos tipos de malware:

- Backdoor
- Botnet (Zombies)
- Exploit
- Gusano
- Hoax
- Keylogger
- Phishing
- Rogue
- Rootkit
- Spam
- Spyware/Adware
- Troyano

saber más

Algunos tipos de intrusos informáticos:

- Hacker
- Cracker
- Lamer
- CopyHacker
- Bucanero
- Phreaker
- Newbie
- Script Kiddie

saber más

El ataque cometido por parte de un *hacker* que utiliza ordenadores intermediarios para ocultar la propia identidad (IP) hasta llegar a su objetivo es un ataque indirecto.

Impactos

Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser **cuantitativos**, si los perjuicios pueden cuantificarse económicamente, o **cualitativos,** si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

3.2. Proceso del análisis de riesgos

Para implantar una política de seguridad en un sistema de infor mación es necesario seguir un esquema lógico.

- Hacer inventario y valoración de los activos.
- Identificar y valorar las amenazas que puedan afectar a la seg uridad de los activos.
- Identificar y evaluar las medidas de seguridad existentes.
- Identificar y valorar las vulnerabilidades de los activos a la s amenazas que les afectan.
- Identificar los objetivos de seguridad de la organización.
- Determinar sistemas de medición de riesgos.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección.

caso **práctico** inicial

Analizar los riesgos de un sistema de información requiere un proceso secuencial de análisis de activos, sus vulnerabilidades, amenazas que existen, medidas de seguridad existentes, impacto que causaría un determinado ataque sobre cualquiera de los activos, objetivos de seguridad de la empresa y selección de medidas de protección que cubran los objetivos.

ACTIVIDADES

11. La ventana de un centro de cálculo en donde se encuentran la mayor parte de los ordenadores y el servidor de una organización se quedó mal cerrada. Durante una noche de tormenta, la ventana abierta ¿constituye un riesgo, una amenaza o una vulnerabilidad? Razona la respuesta.

12. Teniendo en cuenta las propiedades de integridad, disponibilidad y confidencialidad, indica cuáles de estas propiedades se verían afectadas por:

a) Una amenaza de interrupción.

b) Una amenaza de interceptación.

c) Una amenaza de modificación.

d) Una amenaza de fabricación.

13. Pon un ejemplo de cómo un sistema de información podría ser seriamente dañado por la presencia de un factor que se considera de poca relevancia y que explique de alguna manera que «La cadena siempre se rompe por el eslabón más débil».

14. ¿Qué elementos se estudian para hacer un análisis de riesgos?

4. Control de riesgos

Una vez que se ha realizado el análisis de riesgos se tiene que determinar cuáles serán los **servicios** necesarios para conseguir un sistema de información seguro (epígrafe 2.3). Para poder dar esos servicios será necesario dotar al sistema de los **mecanismos** correspondientes.

4.1. Servicios de seguridad

Integridad

Asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

↑ Confidencialidad.

Confidencialidad

Proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Disponibilidad

Permitirá que la información esté disponible cuando lo requieran las entidades autorizadas.

↑ Autenticación.

Autenticación (o identificación)

El sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o que genera una determinada información es quien di ce ser. Solo cuando un usuario o entidad ha sido autenticado,podrá tener autorización de acceso. Se puede exigir autenticación en la entidad de origen de la información, en la de destino o en ambas.

No repudio (o irrenunciabilidad)

Proporcionará al sistema una serie de evidencias irrefutables de la autoría de un hecho.

El **no repudio** consiste en no poder negar haber emitido una información que sí se emitió y en no poder negar su recepción cuando sí ha sido recibida.

De esto se deduce que el **no repudio** puede darse:

- **En origen.** El emisor no puede negar el envío porque el receptor tiene pruebas certificadas del envío y de la identidad del emisor.Las pruebas son emitidas por el propio emisor.
- **En destino.** En este caso es el destinatario quien no puede negar haber recibido el envío ya que el emisor tienepruebas infalsificables del envío y de la identidad del destinatario. Es el receptor quien crea las pruebas.

Control de acceso

Podrán acceder a los recursos del sistema solamente el personaly usuarios con autorización.

caso práctico inicial

Cuando se realiza un análisis de riesgos, hay que detectar qué servicios de seguridad cumple el sistema de información y cuáles quedan descubiertos o incompletos para poder aplicar los mecanismos necesarios que aseguren la consecución de los objetivos de seguridad de la organización

4.2. Mecanismos de seguridad

Según la función que desempeñen los mecanismos de seguridad pue den clasificarse en:

- **Preventivos.** Actúan antes de que se produzca un ataque. Su misión es evitarlo.
- **Detectores.** Actúan cuando el ataque se ha producido y antes de que cause daños en el sistema.
- **Correctores.** Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

caso **práctico** inicial

Hablamos de seguridad física o seguridad lógica según que el mecanismo utilizado para ofrecer seguridad sea físico o lógico.

Cada mecanismo ofrece al sistema uno o más **servicios** de los especificados en el epígrafe anterior.

Existen muchos y variados mecanismos de seguridad. En esta sección se mencionan los más habituales, que se detallarán en otras unidades didácticas.

La elección de mecanismos de seguridad depende de cada sistema de información, de su función, de las posibilidades económicas de la organización y de cuáles sean los riesgos a los que esté expuesto el sistema.

caso **práctico** inicial

Los mecanismos físicos o lógicos de seguridad tienen como misión prevenir, detectar o corregir ataques al sistema, asegurando que los servicios de seguridad queden cubiertos.

Seguridad lógica

Los mecanismos y herramientas de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa.

- **Control de acceso** mediante nombres de usuario y contraseñas.
- **Cifrado de datos** (encriptación). Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Emisor y receptor son conocedores de la clave y a la llegada del mensaje se produce el descifrado. El cifrado de datos fortalece la confidencialidad.
- **Antivirus.** Detectan e impiden la entrada de virus y otro software malicioso. En el caso de infección tienen la capacidad de eliminarlos y de corregir los daños que ocasionan en el sistema. Preventivo, detector y corrector. Protege la integridad de la información.
- **Cortafuegos** (*firewall*). Se trata de uno o más dispositivos de software, de hardware o mixtos que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información.
- **Firma digital.** Se utiliza para la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos (por ejemplo, gestiones en oficinas virtuales). Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o del documento. Protege la integridad y la confidencialidad de la información.
- **Certificados digitales.** Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien dice ser, avalada por la verificación de su clave pública. Protege la integridad y la confidencialidad de la información.

↑ Antivirus, seguridad lógica. Previenen, detectan y corrigen ataques al sistema informático.

↑ Firma digital.

Las redes inalámbricas (WiFi) necesitan precauciones adicionales para su protección:

- **Usar un SSID** ***(Service Set Identifier)***, es decir, darle un nombre a la red, preferiblemente uno que no llame la atención de terceros que detecten esta red entre las disponibles. Cambiar con cierta frecuencia el SSID.
- **Protección de la red mediante claves encriptadas WEP** ***(Wired Equivalent Privacy)*** o **WPA** ***(WiFi Protected Access)***. La clave WEP consume más recursos y es más fácilmente descifrable que la WPA y debería cambiarse con frecuencia. La WPA es de encriptación dinámica y mucho más segura al ser más difícil de descifrar. Cambiar periódicamente la contraseña de acceso a la red.
- **Filtrado de direcciones MAC** ***(Media Access Control)***. Es un mecanismo de acceso al sistema mediante hardware, por el que se admiten solo determinadas direcciones, teniendo en cuenta que cada tarjeta de red tiene una dirección MAC única en el mundo. Puede resultar engorroso de configurar y no es infalible puesto que es posible disfrazar la dirección MAC real.

Detector de humos

SAI (Sistema de alimentación ininterrumpida)

↑ Elementos de seguridad física.

Seguridad física

Son tareas y mecanismos físicos cuyo objetivo es proteger al sistema (y, por tanto indirectamente a la información) de peligros físicos y lógicos.

- **Respaldo de datos.** Guardar copias de seguridad de la información del sistema en lugar seguro. Disponibilidad.
- **Dispositivos físicos** de protección, como pararrayos, detectores de humo y extintores, cortafuegos por hardware, alarmas contra intrusos, sistemas de alimentación ininterrumpida (para picos y cortes de corriente eléctrica) o mecanismos de protección contra instalaciones. En cuanto a las personas, acceso restringido a las instalaciones; por ejemplo, mediante vigilantes jurados o cualquier dispositivo que discrimine la entrada de personal a determinadas zonas.

ACTIVIDADES

15. Investiga el término *war driving,* que también puede expresarse como *wardriving* o *war xing*. ¿Crees que el *war driving* constituye un riesgo contra la confidencialidad?

16. ¿Qué relación hay entre servicios de seguridad y mecanismos de seguridad?

17. ¿Qué es el SSID de una red WiFi?

18. ¿Podrías explicar qué significa encriptar un mensaje? Inventa un sencillo sistema de encriptación (codificación). Imagina que envías a otra persona unas palabras codificadas según tu sistema inventado. ¿Qué necesita tener o saber la persona que recibe tu mensaje para poder descifrarlo?

19. De los siguientes dispositivos indica cuáles son preventivos, detectores o correctores:

a) Cortafuegos *(firewall).*

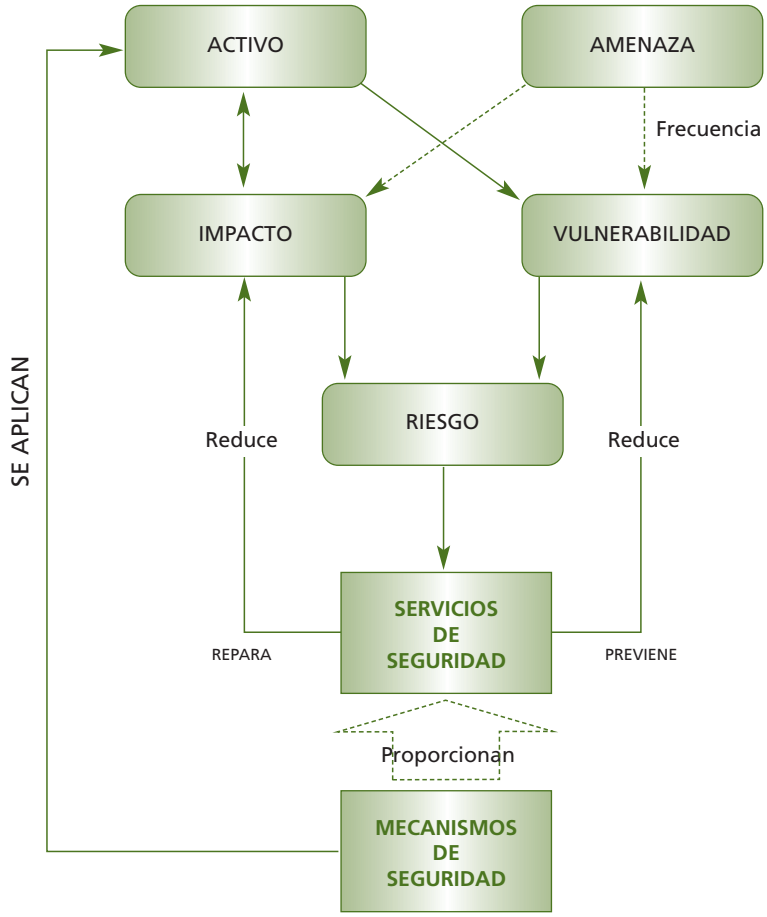
b) Antivirus.

c) Extintor de fuegos.

d) Detector de humos.

e) Firma digital.

En este gráfico se puede observar claramente la relación entre mecanismos y servicios de seguridad, y de ambos sobre los activos y los peligros que los acechan.



caso **práctico** inicial

Los mecanismos de seguridad proporcionan servicios de seguridad que reducen tanto las vulnerabilidades del sistema como la intensidad del impacto de posibles ataques a los activos.

ACTIVIDADES

20. Imagina esta situación: Quieres presentar a tu jefe una brillante idea que puede interesar a la competencia, pero te encuentras de fin de semana en un pueblecito donde los teléfonos móviles no funcionan, por suerte te has llevado tu portátil y el hotel rural donde te encuentras alojado dispone de servicio de internet. Así que decides enviarle un correo electrónico pero sin encriptar. Explica los peligros de este procedimiento.

21. Investiga qué es la esteganografía.

22. ¿Cómo escogerías una clave segura de acceso al ordenador de una empresa donde se guardan datos confidenciales de clientes?

23. Trabajas como técnico de informática y te llega una llamada de una oficina. Un empleado hacía cada semana una copia de seguridad de la carpeta Documentos Importantes. La copia la guardaba en otra partición del mismo disco duro. Una tormenta eléctrica ha dañado el disco y un experto en informática no ha hallado modo de restablecer su funcionamiento. Te piden que te acerques a la oficina para ver si existe la posibilidad de recuperar al menos los datos.

a) ¿Podrás recuperar los datos originales?

b) En su defecto, ¿podrán recuperarse los que hay en la copia de seguridad?

c) A tu juicio, ¿el empleado ha cometido alguna imprudencia con la copia de seguridad?

4.3. Enfoque global de la seguridad

recuerda

La seguridad de la información implica a todos los niveles que la rodean:

1. Edificio y habitaciones
2. Hardware y red interna
3. Sistema operativo y software
4. Conexión a Internet

En cada nivel intervienen personas.

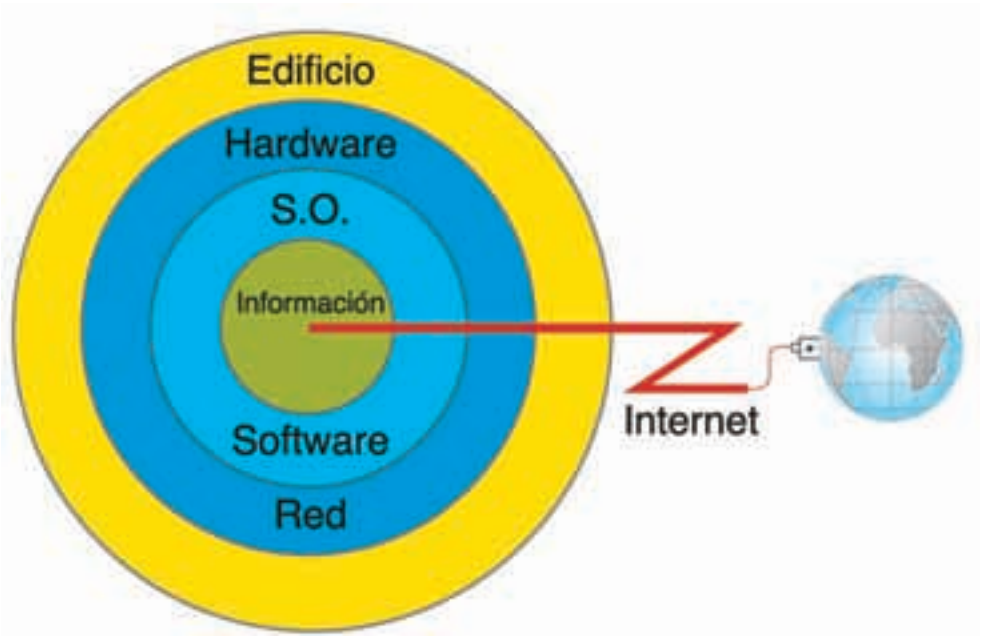
La información es el núcleo de todo sistema de información. Para proteger sus propiedades de integridad, disponibilidad y confidencialidad es necesario tener en cuenta a los niveles que la rodean para dotarlos de mecanismos y servicios de seguridad.

Desde el exterior hasta llegar a la información, se pueden definir estos niveles:

- La ubicación física. Edificio, planta o habitaciones, por ser el lugar físico en donde se encuentran ubicados los demás niveles.
- El hardware y los componentes de la red que se encuentran en el interior del entorno físico, porque contienen, soportan y distribuyen la información.
- El sistema operativo y todo el software, porque gestiona la información.
- La conexión a internet, por ser la vía de contacto entre el sistema de información y el exterior.
- La información.

Observa la figura siguiente para comprobar que la conexión a internet atraviesa los distintos niveles hasta llegar a la información: En el edificio habrá antenas, cableado en los muros, etc. Entre el hardware contamos con routers, switches, ordenadores, servidores, periféricos, etc. El sistema operativo y el software gestionan los accesos a internet. La información es el bien preciado que no se debe descuidar, pues desde internet solamente se podrá acceder a una parte de ella y siempre que los usuarios tengan autorización.

Una vez más aludimos al personal de la empresa que puede actuar en todos los niveles o en parte de ellos y por lo tanto es un factor a tener en cuenta.



5. Herramientas de análisis y gestión de riesgos

5.1. Política de seguridad

Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección.

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización.

No todas las políticas de seguridad son iguales. El contenido depende de la realidad y de las necesidades de la organización para la que se elabora.

Existen algunos estándares de políticas de seguridad por países y por áreas (gobierno, medicina, militar…), pero los más internacionales son los definidos por la ISO (***I**nternational **O**rganization for **S**tandardization*).

Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de información, generalmente englobados en cuatro grupos:

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- Relacionar todas las medidas de seguridad que deben 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 los diferentes departamentos de la organización
- Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- Definir un plan de contingencias.

caso práctico inicial

Los objetivos y normas de seguridad están recogidos en la política de seguridad de la organización. Para la consecución de objetivos, el personal debe estar informado de cuál es la política de seguridad de la empresa.

EJEMPLOS DE HERRAMIENTAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

MAGERIT. Es una metodología de análisis y gestión de riesgos de los sistemas de información. En inglés *Methodology for Information Systems Risk Analysis and Management*.

PILAR. Es un procedimiento informático-lógico para el análisis y gestión de riesgos, que sigue la metodología MAGERIT. De uso exclusivo de la Administración Pública Española.

5.2. Auditoría

caso práctico inicial

La auditoría, mediante pruebas analíticas sobre los activos y procesos que desarrolla la organización, descubre vulnerabilidades, establece medidas de protección y analiza periódicamente el sistema de información para detectar los riesgos no contemplados o de nueva aparición.

El estudio puede realizarse mediante software específico para auditoría de sistemas.

La auditoría es un análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan. Su finalidad es verificar que se cumplen los objetivos de la **política de seguridad** de la organización. Proporciona una imagen real y actual del estado de seguridad de un sistema de información.

Tras el análisis e identificación de vulnerabilidades, la persona o equipo encargado de la auditoría emite un **informe** que contiene, como mínimo:

- Descripción y características de los **activos** y **procesos** analizados.
- Análisis de las **relaciones y dependencias** entre activos o en el proceso de la información.
- Relación y evaluación de las **vulnerabilidades** detectadas en cada activo o subconjunto de activos y procesos.
- Verificación del cumplimiento de la **normativa** en el ámbito de la seguridad.
- Propuesta de **medidas** preventivas y de corrección.

Para evaluar la seguridad de un sistema de información se necesitan herramientas de análisis:

- **Manuales.** Observación de los activos, procesos y comportamientos, mediciones, entrevistas, cuestionarios, cálculos, pruebas de funcionamiento.
- **Software específico para auditoría.** Se le reconoce por las siglas CAAT (***C**omputer **A**ssisted **A**udit **T**echniques*). Los CAATS son herramientas de gran ayuda para mejorar la eficiencia de una auditoría, pudiendo aplicarse sobre la totalidad o sobre una parte del sistema de información. Proporcionan una imagen en tiempo real del sistema de información, realizan pruebas de control y emiten informes en los que señalizan las vulnerabilidades y puntos débiles del sistema, así como las normativas que podrían estar incumpliéndose.

saber más

Software de auditoría

- CaseWare
- WizSoft
- Ecora
- ACL

La auditoría puede ser **total,** sobre todo el sistema de información, o **parcial,** sobre determinados activos o procesos.

La auditoría de un sistema de información puede realizarse:

- Por personal capacitado perteneciente a la propia empresa.
- Por una empresa externa especializada.

ACTIVIDADES

24. Investiga qué es un test de intrusión.

25. Tu jefe te dice que ha detectado que el rendimiento de los trabajadores ha bajado considerablemente desde que la empresa tiene acceso a internet. Te pide que le propongas una solución.

26. En tu empresa acaban de crear unas claves de seguridad para los empleados. Dichas claves se envían por correo electrónico. ¿Esto es desconocimiento de las prácticas de seguridad?

5.3. Plan de contingencias

Determinadas amenazas a cualquiera de los activos del sistema de información pueden poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.

El plan de contingencias consta de tres subplanes independientes:

- **Plan de respaldo.** Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en lugar seguro copias de seguridad de la información, instalar pararrayos o hacer simulacros de incendio.
- **Plan de emergencia.** Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse. Por ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.
- **Plan de recuperación.** Indica las medidas que se aplicarán cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento del sistema y de la organización. Por ejemplo, tener un lugar alternativo donde continuar la actividad si el habitual hubiese sido destruido, sustituir el material deteriorado, reinstalar aplicaciones y restaurar copias de seguridad.

La elaboración del plan de contingencias no puede descuidar al personal de la organización, que estará informado del plan y entrenado para actuar en las funciones que le hayan sido encomendadas en caso de producirse una amenaza o un impacto.

caso práctico inicial

El plan de contingencias contiene medidas preventivas, paliativas y de recuperación de desastres.

El personal no solamente debe estar informado del plan de contingencias sino preparado para actuar ante un peligro o un desastre. Ejemplo: simulacros de incendio.

ACTIVIDADES

27. El hecho de preparar un plan de contingencias, ¿implica un reconocimiento de la ineficiencia en la gestión de la empresa?

28. ¿Cuál es la orientación principal de un plan de contingencia?

29. Investiga: diferencias entre redes cableadas y redes inalámbricas WIFI.

30. ¿En qué se basa la recuperación de la información?

31. Tu jefe te pide que le hagas una buena política de copias de seguridad para que sea seguida por todos los trabajadores de la empresa. ¿Qué deberá contemplar?

32. Trabajas en una empresa donde además de la oficina central, hay una red de oficinas por varias ciudades. Se elabora un plan de contingencias exclusivamente para la oficina central, ¿es esto correcto?

33. En tu empresa se desarrolla un plan de contingencias que entre otras muchas situaciones, cubre las siguientes: un corte en la corriente eléctrica, el sol pasando a través de un cristal en pleno agosto, derramar una bebida en el teclado o sobre el monitor, olvidarse el portátil en un taxi, el robo del ordenador.

¿Crees que cubrir estos puntos es acertado?

5.4. Modelos de seguridad

Un modelo de seguridad es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información. Al decir formal queremos expresar que estará redactado fundamentalmente en términos técnicos y matemáticos.

Clasificación

En relación a las funciones u operaciones sobre las que se ejerce mayor control podemos clasificar los modelos de seguridad en tres grandes grupos:

- **Matriz de acceso.** Este modelo considera tres elementos básicos: sujeto, objeto y tipo de acceso. Un sujeto tiene autorización de acceso total o parcial a uno o más objetos del sistema. Aplicable a cualquier sistema de información, controla tanto la confidencialidad como la integridad de los datos.
- **Acceso basado en funciones de control** (RBAC –***R**ole-**A**ccess **B**ase **C**ontrol*–). Puede considerarse una modalidad del de matriz de acceso, pero, en este caso, el acceso no se define en función de quién es el sujeto, sino de qué función tiene. Por ejemplo, un determinado individuo puede ser alumno de una universidad en cuanto que está estudiando una carrera, pero también puede ser profesor de la universidad en otra especialidad distinta de la misma universidad. Tratándose del mismo individuo, en calidad de profesor tendrá un tipo de acceso al sistema y en calidad de alumno tendrá otro. También controla la confidencialidad y la integridad de los datos.
- **Multinivel.** Este modelo se basa en la jerarquización de los datos (todos los datos son importantes pero unos son más privados que otros. Por ejemplo, el nivel de protección de datos personales ha de ser superior que los nombres de los artículos con los que comercia una empresa). Los usuarios tendrán acceso a un nivel u otro de la jerarquía en función de las autorizaciones que les hayan sido dadas. Este nivel controla el flujo de datos entre los niveles de la jerarquía. Ejemplos de este grupo son el modelo *Bell-LaPadula* (controla la confidencialidad) y el modelo *Biba* (controla la integridad).

ACTIVIDADES

34. ¿Una misma política de seguridad puede servir a todo tipo de empresas?

35. ¿De qué modo debe ser redactada la política de seguridad de una organización?

36. Define con tus propias palabras qué es un plan de contingencias.

37. Investiga en internet sobre empresas especializadas en auditorías de sistemas de información (sugerencias: Hipasec, Audisis). Escoge una de estas empresas y contesta las siguientes preguntas:

a) ¿En qué fases realiza la auditoría?

b) ¿Qué tipos de auditoría realiza?

c) ¿Ofrece revisiones periódicas del sistema?

38. Investiga en internet para encontrar el software de auditoría: CaseWare, WizSoft, Ecora, ACL, AUDAP u otros. Escoge uno o varios y haz una lista de las operaciones que realiza para llevar a cabo la auditoría.

39. Averigua qué información tiene wikipedia sobre el modelo de seguridad Bell-LaPadula. Escribe la definición que hace del modelo.

PRÁCTICA PROFESIONAL

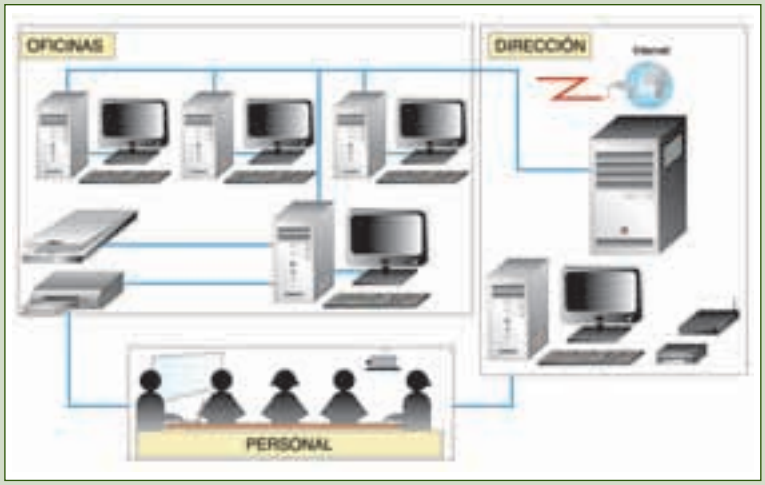
Estudio de la seguridad en una empresa

Empresa: asesoría laboral y fiscal.

Instalaciones: una oficina, una sala de reuniones y el despacho de dirección. Protección contra incendios y alarma contra intrusos.

Oficina: cuatro ordenadores en la oficina. Uno de ellos tiene conectados dos periféricos: una impresora y un escáner. Todos los ordenadores van conectados mediante cable a un servidor.

Dirección: un ordenador con conexión inalámbrica a la red. Un servidor conectado a internet. Además, en dirección se encuentra el archivo de todas las copias de seguridad de los datos, que se generan una vez al día.



Sala de reuniones: mesa y sillas para reuniones, un portátil, pantalla y proyector.

Recursos humanos: cinco personas, de ellas cuatro trabajan en la oficina; la directora de la asesoría, en su despacho.

Software: sistemas operativos, aplicaciones específicas para gestorías y asesorías, antivirus, *firewall*.

Situación: la asesoría tiene definida su política de seguridad, conocida por todo el personal. Recientemente le ha sido realizada una auditoría informática, y el estado de seguridad ha sido calificado como óptimo. Sin embargo, el ordenador de la dirección, debido a un pico de corriente, ha sufrido daños en la placa base y el disco duro. Ambos elementos deben ser reemplazados. La información contenida en el disco duro había sido previamente copiada y se encuentra archivada.

Resuelve

Con los conocimientos que posees tras haber estudiado esta unidad:

1. Enumera los activos del sistema de información de la asesoría.
2. ¿Se ha producido algún ataque? En caso afirmativo, responde cuál ha sido.
3. ¿Crees que ha sido importante para la empresa el impacto por los daños en la placa base y el disco duro? Comenta tu impresión.
4. Investiga si existe algún medio para evitar que los picos de corriente puedan dañar equipos o dispositivos físicos de un sistema informático.
5. El disco duro inutilizado contenía información personal y fiscal de clientes de la asesoría. Se ha decidido tirarlo a la basura, pero una empleada dice que ese método no es seguro. Haz tus investigaciones y comenta si has averiguado que la empleada está o no en lo cierto.

MUNDO LABORAL

Las personas son el eslabón débil en la ciberseguridad

La popularidad de Facebook y otros sitios muy visitados de redes sociales ha dado a los *hackers* nuevas vías para robar dinero e información, dijo la compañía de seguridad Sophos en un reporte publicado el miércoles.

Cerca de la mitad de las compañías bloquea parcial o completamente el acceso a las redes sociales debido a la preocupación por ciber-incursiones a través de esos sitios, de acuerdo al estudio.

«Los resultados de las investigaciones también revelaron que un 63 por ciento de los administradores de sistemas están preocupados porque sus empleados comparten demasiada información personal a través de los sitios de redes sociales, lo que pone su infraestructura corporativa –y los datos sensibles almacenados en ella– en riesgo», dijo el reporte de Sophos.

Esto ocurre a pesar de años de exhortaciones a los usuarios de computadoras respecto a que deberían mantener su información personal en privado y abstenerse de abrir archivos adjuntos de correos electrónicos provenientes de fuentes no conocidas.

Uno de los resultados es que una cuarta parte de los negocios ha sido afectada por tácticas como el *spam*, el *phishing* o ataques de software malicioso a través de Twitter u otras redes sociales, dijo Sophos.

El *phishing* es el envío de correos electrónicos a través de los cuales los estafadores tratan de convencer a sus potenciales víctimas para que revelen información personal como contraseñas o cuentas bancarias.

Sophos también descubrió que la cantidad de páginas web con software malicioso se cuadruplicó desde principios del 2008, y un 39,6 por ciento de ellas tiene sede en Estados Unidos, que alberga más que cualquier otro país. China es el segundo, con 14,7 por ciento.

Sophos, que tiene sedes en Gran Bretaña y Estados Unidos, es el mayor fabricante de software de capital privado.

Reuters

Reporte de Diane Bartz;
editado en español por Hernán García

http://lta.reuters.com/article/internetNews/idLTASIE56L08920090722

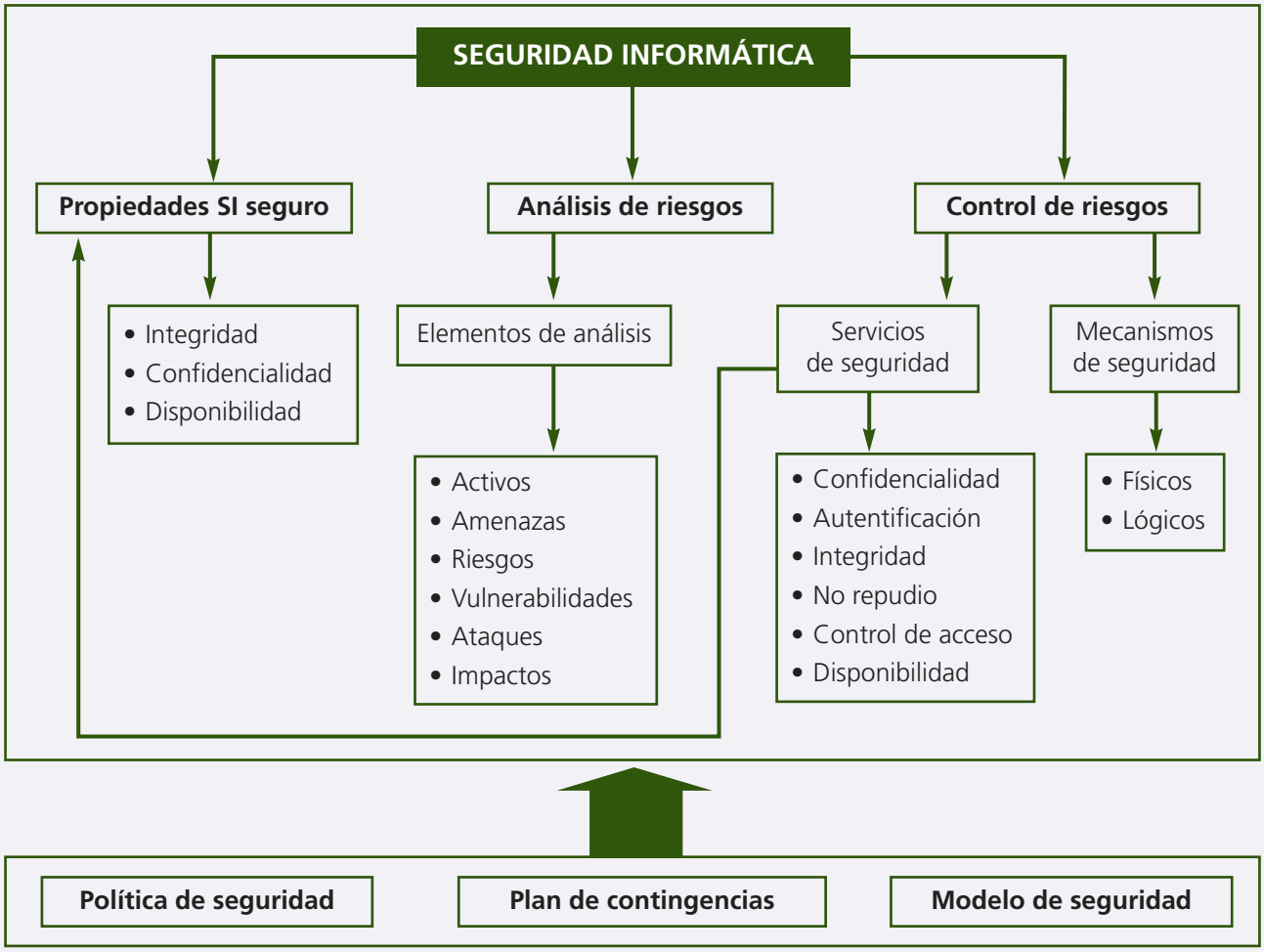
Washington, miércoles 22 de julio de 2009

Actividades

Lee el artículo y en vista de su contenido responde a las siguientes cuestiones:

1. ¿Qué propiedades de seguridad del sistema de información podrían verse vulneradas por negligencias cometidas por empleados de la empresa al publicar sus datos personales en redes sociales?
2. Indica alguna manera de que los administradores de un sistema de información puedan impedir que el personal de la empresa acceda a sitios que podrían poner en peligro las propiedades de seguridad del sistema.
3. ¿Qué proporción de negocios se ven afectados por *spam* o software malicioso debido al uso indebido de redes sociales por parte de los empleados?
4. En tu opinión, ¿consideras cierta la afirmación de que se producen más fallos de seguridad por la intervención humana que por errores en la tecnología?

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. El conjunto de datos organizados que tienen significado se llama:
   a) Recurso.
   b) Actividad.
   c) Software.
   d) Información.
2. Señala cuál de estos elementos no forma parte de un sistema informático:
   a) Router.
   b) Usuario.
   c) Teclado.
   d) Estante.
3. Señala, en la siguiente lista, lo que es un activo:
   a) Inundación.
   b) Riesgo.
   c) Red local.
   d) Política de seguridad.
4. Indica la respuesta correcta que te sugiera la palabra disponibilidad:
   a) Asegura que los datos no han sido modificados.
   b) Protección contra la revelación de datos.
   c) Identifica personas.
   d) Permite el acceso solo a usuarios con autorización.

Soluciones: 1d, 2d, 3c, 4d