U.T.1 Principios de seguridad y alta disponibilidad

Sumario

1 ¿Por qué proteger?

1.1 Introducción

Los usuarios deberían saber que sus máquinas son muy poderosas, pero también muy vulnerables. Es importante reconocerlo, dado que nuestra vida es digital: hablamos por teléfonos móviles, enviamos mensajes con aplicaciones IP, como e-mail, WhatsApp, etc., hacemos compras por Internet, estudiamos por Internet, entramos en contacto con determinada empresas y organizaciones a través de su página web y las empresas realizan entre sí contratos electrónicos sin necesitar una firma en un papel.

Por eso hay que estar preparados para evitar estas situaciones:

- Nuestras conversaciones son personales: nadie más debería poder escucharlas.
- Nuestros mensajes son privados: nadie debería tener acceso a ellos.
- Una compra solo interesa al vendedor y al comprador.
- La información pública en Internet debe estar al alcance de todos.
- Las empresas deben cuidar su imagen: no pueden consentir un ataque a su página web que modifique el contenido, engañando a sus clientes y usuarios.
- Los contratos entre empresas son privados en muchos casos. Nadie externo debe poder alterarlos, ni siquiera conocerlos.

La seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital.

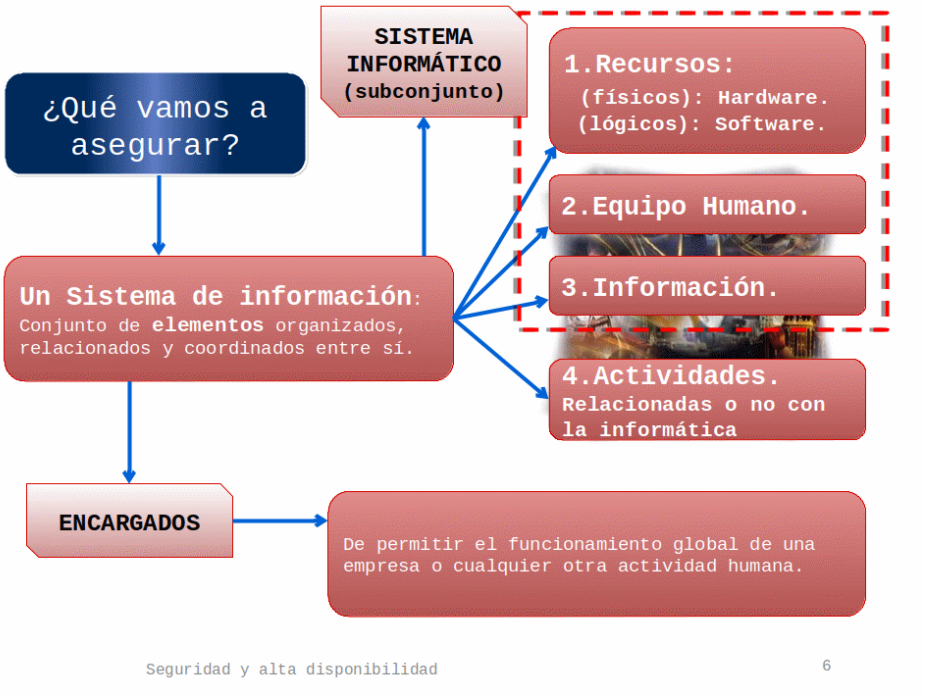
- Las conversaciones por teléfono móvil van cifradas: aunque otro móvil pueda recibir la misma señal, no puede entender qué están transmitiendo.
- Los mensajes se almacenan en el servidor de correo y, opcionalmente, en el cliente de correo que ejecuta en mi ordenador. Debemos proteger esos equipos, así como la comunicación entre ambos.
- La navegación por la web del vendedor puede ser una conexión no cifrada, pero cuando se utiliza el carrito debemos pasar a servidor seguro. La web del vendedor debe estar disponible a todas horas: hay que protegerla frente a caídas de tensión, cortes de red, accidentes o sabotajes de sus instalaciones.
- Los servidores de información de una red mundial deben estar disponibles a todas horas.
- Las empresas deben restringir el acceso a las partes protegidas de su web, como la administración y la edición de contenidos
- Los contratos deben llevar la firma digital de las empresas interesadas y deben almacenarse en discos cifrados con almacenamiento redundante, cuya copia de

seguridad irá también cifrada y se dejará en un edificio diferente, a ser posible en otra ciudad.

A pesar de toda nuestra preocupación y todas las medidas que tomemos, **la seguridad completa es imposible**. Debemos asumir que hemos desplegado la máxima seguridad posible con el presupuesto asignado y la formación actual de nuestros técnicos y usuarios. Por otra parte, podemos estar seguros de que en nuestra casa o en nuestra empresa estamos aplicando todas las medidas; pero no sabemos qué hacen las otras personas con las que nos comunicamos. En el ámbito personal, posiblemente enviamos imágenes a alguien que no sabe que tiene un troyano en su ordenador.

En el fondo, todo es información: sean los 140 caracteres de un tweet, sean ficheros de varios megabytes, están en nuestro equipo y alguien puede intentar obtenerlos. **La clave es la motivación: quién está interesado en nuestra información**. Es poco probable que algún superhacker intente entrar en nuestro ordenador portátil, seguramente no le costaría mucho, pero el esfuerzo no le merece la pena. Las empresas sí son mucho más atractivas para estas actividades delictivas, por lo que existen las auditorías de seguridad y los tiger teams: contratamos a una empresa externa especializada en seguridad informática para que revise nuestros equipos y nuestros procedimientos.

1.2 ¿Que vamos a proteger?



1.2.1 Equipos

Es fundamental que no se puedan sustraer, ni el equipo ni sus piezas, principalmente el disco duro, pero también el dispositivo donde se hace la copia de seguridad de ese disco.

En el caso de los portátiles no podemos evitar que salgan de la empresa. Pero sí debemos vigilar que esos ordenadores apliquen cifrado en el disco duro y tengan contraseñas actualizadas.

Es importante que no se puedan introducir nuevos equipos no autorizados.

Aplicaremos mantenimiento preventivo para evitar averías.

1.2.2 Aplicaciones

Los ordenadores de una empresa deben tener las aplicaciones estrictamente necesarias para llevar a cabo el trabajo asignado, debemos evitar instalar software extra (ya sea intencionadamente o no) porque puede tener vulnerabilidades. Cuando una empresa adquiere un nuevo equipo, el personal de sistemas procede a maquetarlo: instala las aplicaciones utilizadas en esa empresa, con la configuración particular de esa empresa. Incluso puede llegar a sustituir el sistema operativo que traía el equipo.

Los objetivos son ahorrar al usuario la tarea de instalar y configurar las aplicaciones, asegurar que el software instalado responde a las licencias compradas en la empresa y homogeneizar el equipamiento, de manera que solo tendremos que enfrentarnos a los problemas en una lista reducida de configuraciones de hardware.

Tanto si es intencionada como si no, el antivirus será una barrera a la instalación de aplicaciones no autorizadas, y la ausencia de privilegios de administración también ayudará. Pero conviene aplicar otras medidas para no ponerlos a prueba, como desactivar el mecanismo de autoarranque de aplicaciones desde CD o USB e incluso deshabilitar estas unidades lectoras.

1.2.3 Datos

Hay que protegerlos por dos motivos: si desaparecen, la empresa no puede funcionar con normalidad, y si llegan a manos de la competencia, la estrategia y el futuro de la compañía están en riesgo. Las empresas modernas responden al esquema de «oficina sin papeles»: están informatizados todos los datos que entran, los generados internamente y los que comunicamos al exterior.

La infraestructura necesaria es amplia y compleja porque los niveles de seguridad son elevados:

- Todos los equipos deben estar protegidos contra software malicioso que pueda robar datos o alterarlos.
- El almacenamiento debe ser redundante.

- El almacenamiento debe ser cifrado. Si, por cualquier circunstancia, perdemos un dispositivo de almacenamiento, los datos que contenga deben ser inútiles para cualquiera que no pueda descifrarlos.

1.2.4 Comunicaciones

Los datos no suelen estar recluidos siempre en la misma máquina: salen con destino a otro usuario que los necesita. Esa transferencia también hay que protegerla. **Debemos utilizar canales cifrados, incluso aunque el fichero de datos que estamos transfiriendo ya esté cifrado.**

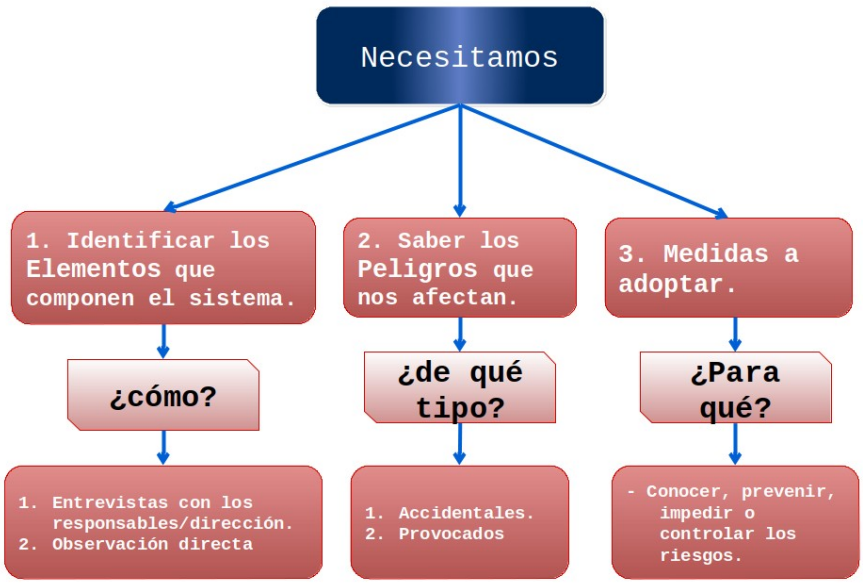
Además de proteger las comunicaciones de datos, también debemos controlar las conexiones a la red de la empresa. Con la expansión del teletrabajo, las redes de las empresas necesitan estar más abiertas al exterior, luego estarán más expuestas a ataques.

El peligro también está en la propia oficina: no puede ser que cualquier visitante entre en nuestra red con solo conectar su portátil a una toma de la pared o a través del wifi de la sala de espera.

También se deberá evitar la llegada de correo no deseado (spam) y publicidad en general.

La tendencia actual en las empresas es migrar sus sistemas a Internet mediante el cloud computing, desplazando toda su infraestructura informática a servidores virtuales con conexión a Internet. Sea cual sea el grado de adopción de cloud computing en una empresa, la primera premisa debe ser la seguridad en las comunicaciones, porque todos los servicios están en máquinas remotas a las que llegamos atravesando redes de terceros.

1.3 Proceso de protección.



2 Seguridad física/lógica, activa/pasiva

2.1 Seguridad física

La seguridad física cubre todo lo referido a los equipos informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red.

Las amenazas contra la seguridad física son:

- Desastres naturales. Los tendremos en cuenta para ubicar el emplazamiento del CPD donde alojamos los principales servidores de la empresa.
- Robos. Debemos proteger el acceso al CPD mediante múltiples medidas: vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc.
- Fallos de suministro. Son recomendables unas baterías o un grupo electrógeno por si falla la corriente, una segunda conexión a Internet como línea de backup para estar protegidos ante un corte en la calle.
- Amenazas ocasionadas por el hombre.

2.1.1 Peligros

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

2.1.1.1 Incendios.

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.

- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Seguridad del Equipamiento

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18° C y el limite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

2.1.1.2 Inundaciones

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Esta es una de las causas de mayores desastres en centros de cómputos. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

2.1.1.3 Condiciones Climatológicas.

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

2.1.1.4 Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

2.1.1.5 Señales de Radar

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años.
Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor.
Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

2.1.1.6 Instalaciones Eléctricas

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta es una de las principales áreas a considerar en la seguridad física.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

- **Picos y Ruidos Electromagnéticos**

  Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

- **Cableado**

  Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxil o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

  Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

  - Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
  - Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
  - Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

  En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

  El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

  - Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
  - Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

  Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

  - **Cableado de Alto Nivel de Seguridad**

  Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y

monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

2.1.1.7 Ergometría

"La Ergonomía es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible."

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

2.1.2 Acciones Hostiles

2.1.2.1 Robo

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.

Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora.

El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro

2.1.2.2 Fraude

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

2.1.2.3 Sabotaje

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han

encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

2.1.3 Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

2.1.3.1 Utilización de Guardias

2.1.3.2 Utilización de Detectores de Metales

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

2.1.3.3 Utilización de Sistemas Biométricos

Definimos a la Biometría como "la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos".

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

Los Beneficios de una Tecnología Biométrica

Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años,

el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

- **Emisión de Calor**

  Se mide la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.

- **Huella Digital**

  Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

  Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Está aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

- **Verificación de Voz**

  La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.).

  Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

- **Verificación de Patrones Oculares**

  Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

  Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

- **Verificación Automática de Firmas (VAF)**

  En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas.

  Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

  La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir.

La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.

El equipamiento de colección de firmas es inherentemente de bajo costo y robusto.

Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

2.1.3.4 Protección Electrónica

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, estos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

- **Barreras Infrarrojas y de Micro-Ondas**

  Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa.

  Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

  Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

  Las microondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

  Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

  Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

- **Detector Ultrasónico**

  Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

- **Detectores Pasivos Sin Alimentación**

  Estos elementos no requieren alimentación extra de ningún tipo, sólo van conectados a la central de control de alarmas para mandar la información de control. Los siguientes están incluidos dentro de este tipo de detectores:

  - Detector de aberturas: contactos magnéticos externos o de embutir.
  - Detector de roturas de vidrios: inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable.
  - Detector de vibraciones: detecta golpes o manipulaciones extrañas sobre la superficie controlada.

- **Sonorización y Dispositivos Luminosos**

  Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc.

  Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

  Se pueden usar transmisores de radio a corto alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

- **Circuitos Cerrados de Televisión**

  Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

  Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se

produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

2.2 Seguridad lógica.

La seguridad lógica se refiere a las distintas aplicaciones que ejecutan en cada uno de estos equipos.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.2.1 Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST)(1) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

2.2.1.1 Identificación/Autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona posee: por ejemplo una tarjeta magnética.
- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían

los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones(Por ejemplo: un servidor RADIUS) sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

2.2.1.2 Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc.

En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

2.2.1.3 Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

2.2.1.4 Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

2.2.1.5 Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
- Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
- Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- Creación: permite al usuario crear nuevos archivos, registros o campos.
- Búsqueda: permite listar los archivos de un directorio determinado.

2.2.1.6 Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

2.2.1.7 Control de Acceso Interno.

Palabras Claves (Passwords)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Es importante usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

- **Sincronización de passwords:** consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.
- **Caducidad y control:** este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado con profundidad en el Capítulo sobre Protección del presente.

Listas de Control de Accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

Límites sobre la Interfase de Usuario

Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

2.2.1.8 Control de Acceso Externo

Dispositivos de Control de Puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

Firewalls o Puertas de Seguridad

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

2.2.1.9 Administración.

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

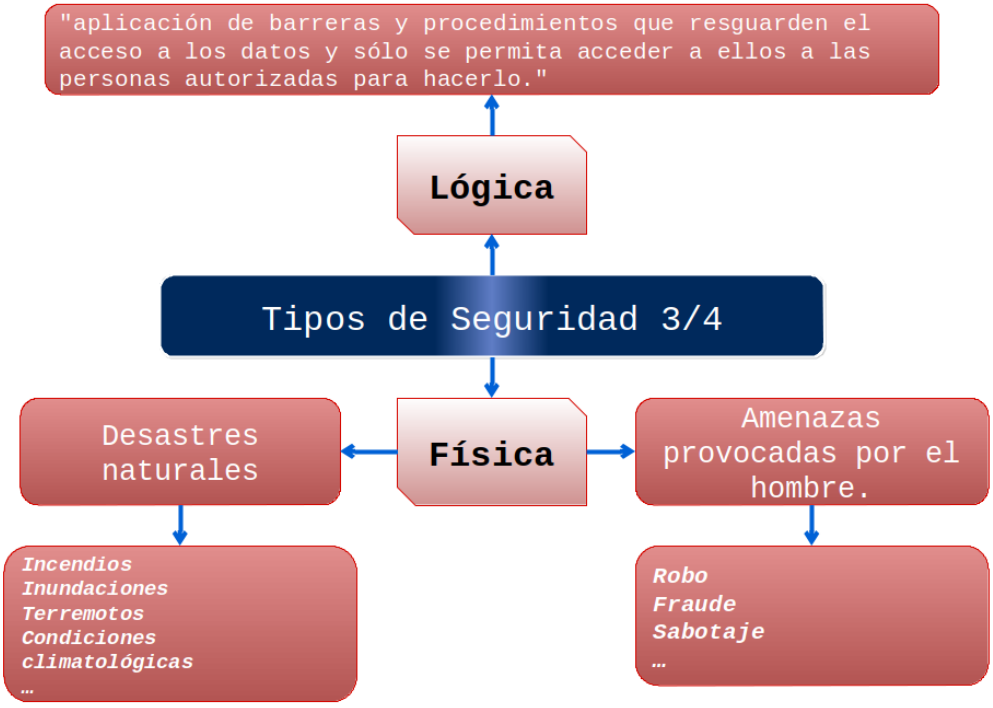
Administración del Personal y Usuarios - Organización del Personal

Este proceso lleva generalmente cuatro pasos:

- Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
- Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
- Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.


"aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."
Lógica
Tipos de Seguridad 3/4
Desastres naturales
Física
Amenazas provocadas por el hombre.
Incendios
Inundaciones
Terremotos
Condiciones climatológicas
…
Robo
Fraude
Sabotaje
…
Seguridad y alta disponibilidad
10

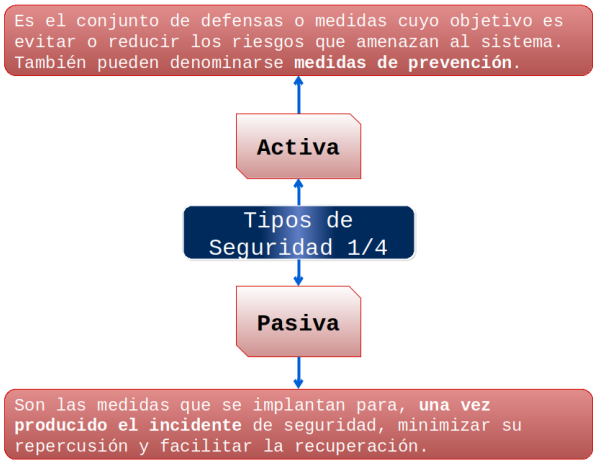

Tipos de Seguridad 4/4
Física
Peligros
Acciones hostiles
Control de accesos
- Incendios.
- Inundaciones.
- Condiciones climatológicas
- Señales de radar.
- Instalaciones eléctricas.
- Ergometría.
- Robo.
- Fraude.
- Sabotaje.
- Guardias.
- Detector de metales.
- Sistemas biométricos.
- Verificación automática de firmas.
- Seguridad con animales.
- Protección electrónica.
Seguridad y alta disponibilidad
11

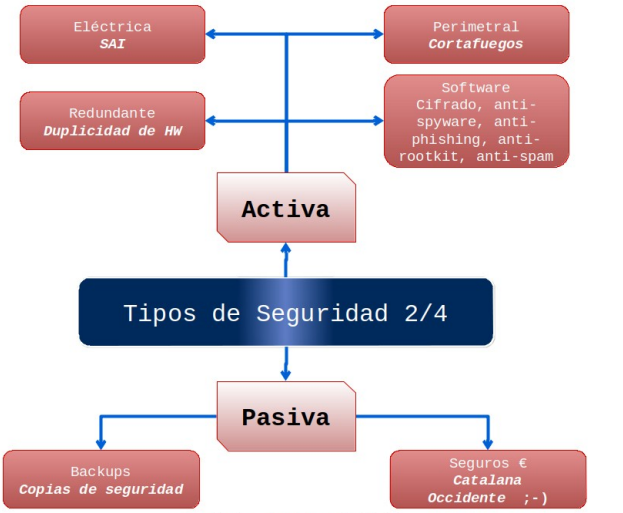
2.3 Seguridad pasiva.

La seguridad pasiva son todos los mecanismos que, cuando sufrimos un ataque, nos permiten recuperarnos razonablemente bien.

2.4 Seguridad activa.

La seguridad activa intenta protegernos de los ataques mediante la adopción de medidas que protejan los activos de la empresa.





3 Sistema seguro

Un sistema es seguro si cumple las siguientes condiciones:

- Confidencialidad
- Disponibilidad
- Integridad
- No repudio

3.1 Confidencialidad

La confidencialidad intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas. Para garantizar la confidencialidad necesitamos disponer de tres tipos de mecanismos:

- **Autenticación.** Intenta confirmar que una persona o máquina es quien dice ser.

  Un esquema muy utilizado para analizar la autenticación es clasificar las medidas adoptadas según tres criterios:

Algo que sabes. Para acceder al sistema necesitas conocer alguna palabra secreta: la típica contraseña.

Algo que tienes. En este caso es imprescindible aportar algún elemento material: generalmente una tarjeta.

Algo que eres. El sistema solicita reconocer alguna característica física del individuo (biometría): huella dactilar, escáner de retina, reconocimiento de voz, etc.

La autenticación será más fiable cuantos más criterios distintos cumpla.

- **Autorización.** Una vez autenticado, los distintos usuarios de la información tendrán distintos privilegios sobre ella: solo lectura, o lectura y modificación.
- **Cifrado.** La información estará cifrada para que sea inútil a quien no supere la autenticación.

3.2 Disponibilidad

La disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido. Para ello se invierte en sobredimensionar los recursos.

3.3 No repudio

El no repudio se refiere a que, ante una relación entre dos partes, intentaremos evitar que cualquiera de ellas pueda negar que participara en esa relación.

3.4 Integridad

El objetivo de la integridad es que los datos queden almacenados tal y como espera el usuario que no sean alterados sin su consentimiento.

4 Tipos de ataques

4.1 Métodos

Una vez que alguien está decidido a atacarnos, puede elegir alguna de estas formas:

- **Interrupción.** El ataque consigue provocar un corte en la prestación de un servicio.
- **Interceptación.** El atacante ha logrado acceder a nuestras comunicaciones y ha copiado la información.
- **Modificación**. Ha conseguido acceder, pero, en lugar de copiar la información, la está modificando.

- **Fabricación.** El atacante se hace pasar por el destino de la transmisión, por lo que puede tranquilamente conocer el objeto de nuestra comunicación y engañarnos para obtener información valiosa.

4.2 Técnicas

Para conseguir su objetivo puede aplicar una o varias de estas técnicas :

4.2.1 Malware

El término Malware se refiere de forma genérica a cualquier software malicioso que tiene por objetivo infiltrarse en un sistema para dañarlo. Aunque se parece a lo que comúnmente se le conoce como virus, el virus es un tipo de malware. Igualmente existen otros como los gusanos, troyanos, etc.

4.2.2 Virus

El virus es un código que infecta los archivos del sistema mediante un código maligno, pero para que esto ocurra necesita que nosotros, como usuarios, lo ejecutemos. Una vez que se ejecuta, se disemina por todo nuestro sistema a donde nuestro equipo o cuenta de usuario tenga acceso, desde sipositivos de hardware hasta unidades virtuales o ubicaciones remotas en una red.

4.2.3 Gusanos

Un gusano es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por las red. A diferencia del virus, no necesita nuestra intervención, ni de un medio de respaldo, ya que pueden transmitirse utilizando las redes o el correo electrónico. Son difíciles de detectar, pues al tener como objetivo el difundirse e infectar a otros equipos, no afectan al funcionamiento normal del sistema.

Su uso principal es el de la creación de botnets, que son granjas de equipos zombies utilizados para ejecutar acciones de forma remota como por ejemplo un ataque DDoS a otro sistema.

4.2.4 Troyanos

Son similares a virus, pero no completamente iguales. Mientras que el virus es destructivo por sí mismo, el troyano lo que busca es abrir una puerta trasera para favorecer la entrada de otros programas maliciosos.

Su nombre es alusivo al “Caballo de Troya” ya que su misión es precisamente, pasar desapercibido e ingresar a los sistemas sin que sea detectado como una amenaza potencial. No se propagan a sí mismos y suelen estar integrados en archivos ejecutables aparentemente inofensivos.

4.2.5 Spyware

Un spyware es un programa espía, cuyo objetivo principal es obtener información. Su trabajo suele ser también silencioso, sin dar muestras de su funcionamiento, para que puedan recolectar información sobre nuestro equipo con total tranquilidad, e incluso instalar otros programas sin que nos demos cuenta de ello.

4.2.6 AdWare

La función principal del adware es la de mostrar publicidad. Aunque su intención no es la de dañar equipos, es considerado por algunos una clase de spyware, ya que puede llegar a recopilar y transmitir datos para estudiar el comportamiento de los usuarios y orientar mejor el tipo de publicidad.

4.2.7 Ransomware

Este es uno de los mas sofisticados y modernos malwares ya que lo que hace es secuestrar datos (encriptándolos) y pedir un rescate por ellos. Normalmente, se solicita una transferencia en bitcoins,la moneda digital, para evitar el rastreo y localización. Este tipo de ciberataque va en aumento y es uno de los más temidos en la Actualidad.

4.2.8 Ingeniería social.

A la hora de poner una contraseña, los usuarios suelen recurrir a palabras conocidas para ellos: el mes de su cumpleaños, el nombre de su calle, su mascota, etc. Si conocemos bien a esa persona, podemos intentar adivinar su contraseña. Otro ejemplo sería pedir a un compañero de trabajo que introduzca su usuario y contraseña, que el nuestro parece que no funciona. En esa sesión podemos aprovechar para introducir un troyano, por ejemplo.

4.2.9 Phishing.

El atacante se pone en contacto con la víctima (generalmente, un correo electrónico) haciéndose pasar por una empresa con la que tenga alguna relación (su banco, su empresa de telefonía, etc.). En el contenido del mensaje intenta convencerle para que pulse un enlace que le llevará a una (falsa) web de la empresa. En esa web le solicitarán su identificación habitual y desde ese momento el atacante podrá utilizarla.

El phishing es un método que igualmente se está sofisticando, tanto en el ámbito particular como en el empresarial. El engaño se busca aportando información más detallada, como aportar el nombre de ejecutivos de la empresa para engañar a los trabajadores de la misma.

4.2.10 Keyloggers.

Un troyano en nuestra máquina puedetomar nota de todas las teclas que pulsamos,buscando el momento en que introducimos un usuarioy contraseña.

4.2.11 Fuerza bruta.

Las contraseñas son un número limitado de caracteres (letras, números y signos de puntuación). Una aplicación malware puede ir generando todas las combinaciones posibles y probarlas una a una; tarde o temprano, acertará.

Contra los ataques de fuerza bruta se recomienda utilizar contraseñas no triviales, cambiar la contraseña con frecuencia, impedir ráfagas de intentos repetidos y establecer un máximo de fallos tras el cual se bloqueará el acceso.

4.2.12 Spoofing.

Alteramos algún elemento hacernos pasar por otra máquina. Por ejemplo, generamos mensajes con la misma dirección que la máquina auténtica.

4.2.13 Sniffing.

El atacante consigue conectarse en el mismo tramo de red que el equipo atacado. De esta manera tiene acceso directo a todas sus conversaciones.

4.2.14 DoS

(Denial of Service, denegación de servicio). Consiste en tumbar un servidor saturándolo con falsas peticiones de conexión.

4.2.15 DDoS

(Distributed Denial of Service, denegación de servicio distribuida). Es el mismo ataque DoS, pero ahora no es una única máquina la que genera las peticiones falsas sino muchas máquinas repartidas por distintos puntos del planeta. Esto es posible porque todas esas máquinas han sido infectadas por un troyano que las ha convertido en ordenadores zombis.

4.2.16 INYECCIÓN SQL

Entre los tipos de ataques en ciberseguridad más conocidos se encuentra la Inyección SQL. Se trata de un método de infiltración de un código intruso que se aprovecha de una vulnerabilidad informática presente en una aplicación. Es decir, se aprovechan de errores de diseño habituales en las páginas web. La amenaza de las inyecciones SQL supone un grave problema de seguridad relacionado con las bases de datos. Se emplean para manipular, robar o destruir datos.

Los ciberdelincuentes son capaces de inyectar consultas SQL maliciosas en el campo de entrada de una web, engañar a la aplicación para que haga uso de los comandos que deseen y acceder a la base de datos que quieran.

Un ataque de inyección SQL puede ralentizar el funcionamiento de una web, el robo, la pérdida o la corrupción de datos, la denegación de acceso de cualquier compañía o incluso la toma del control absoluto del servidor.

4.3 Tipos de atacantes

- **Hackers**: Son normalmente informáticos, que quieren descubrir vulnerabilidades de los sistemas por gusto, sin motivación económica ni dañina.
- **Crackers:** Son las personas que rompen la seguridad del sistema con intención maliciosa, para dañarla u obtener beneficios económicos.
- **Sniffers:** Son expertos en redes que analizan el trafico de la red, para obtener información extrayéndola de los paquetes que se transmiten por la red.
- **LAMMERS:** Son gente joven sin muchos conocimientos informáticos que se consideran a si mismos hackers y presumen de ello.
- **Newbie:** Son hackers novatos.
- **Ciberterrorista:** Son expertos informáticos que trabajan para países u organizaciones como espías si saboteadores informáticos.
- **Programadores de virus:** Estas personas deben ser expertos en programación redes y sistemas., que crean programas dañinos que afectan a aplicaciones y a sistemas.
- **Carders:** Son personas que se dedican a ataques de sistemas de tarjetas como cajeros automáticos.

5 Buenas prácticas

• Localizar los activos que hay que proteger: equipos, aplicaciones, datos y comunicaciones.Revisar la política de copias de seguridad.

• Redactar y revisar regularmente los planes de actuación ante catástrofes, contemplando todaslas posibilidades: ataque intencionado, desastre natural, arranque parcial de servicios.

• No instalar nada que no sea estrictamente necesario, y revisar la configuración de los

sistemas y aplicaciones por si estamos otorgando más permisos de los imprescindibles.

• Estar al día de todos los informes de seguridad que aparezcan. Para ello hay que registrarse en listas de correo sobre seguridad y en las listas de nuestros proveedores.

• Activar los mecanismos de actualización automática de las aplicaciones que tenemos instaladas. Salvo sistemas delicados (tenemos que probar muy bien cada actualización antes de aplicarla), en general los fabricantes liberan actualizaciones que no dan problemas.

• Dar formación a los usuarios para que utilicen la seguridad y la vean como una ayuda, no como un estorbo.

• Revisar los log del sistema (el accounting que hemos visto antes). Algunas herramientas nos ayudan porque recogen los ficheros de log y aplican fácilmente muchos patrones conocidos.

• Considerar la opción de contratar una auditoría externa, porque si hemos cometido un error de concepto, es muy difícil que lo encontremos por nosotros mismos.

• Revisar la lista de equipos conectados: pueden haber introducido equipos no autorizados.

• Revisar la lista de usuarios activos: puede que algún empleado ya no esté en la empresa pero su usuario y todos los privilegios asociados siguen disponibles para él o para alguien de su confianza.

• En aquellos sistemas que lo permitan, configurar el aviso por SMS o correo electrónico para que nos enteremos los primeros de cualquier problema.

6 Legislación sobre seguridad

6.1 LOPD

La Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999, de 13 de diciembre) establece las bases para proteger el tratamiento de los datos de carácter personal de las personas físicas. El Real Decreto 1720/2007, de 21 de diciembre, desarrolla la LOPD para ficheros (automatizados y no automatizados). Define tres tipos de medidas:

- **Nivel básico.** Cualquier fichero de datos de carácter personal. Las medidas de seguridad con estos datos son:
  - Identificar y autenticar a los usuarios que pueden trabajar con esos datos.
  - Llevar un registro de incidencias acontecidas en el fichero.
  - Realizar copia de seguridad como mínimo semanalmente.
- **Nivel medio.** Cuando los datos incluyen información sobre infracciones administrativas o penales, informes financieros y de gestión tributaria y datos sobre la personalidad del sujeto. Las medidas de seguridad incluyen las del nivel básico más:
  - Al menos una vez cada dos años una auditoría externa verificará los procedimientos de seguridad.

    - Debe existir control de acceso físico a los medios de almacenamiento de los datos.
- **Nivel alto.** Son los datos especialmente protegidos: ideología, vida sexual, origen racial, afiliación sindical o política, historial médico, etc. Las medidas de seguridad amplían las de nivel medio:
    - Cifrado de las comunicaciones.
    - Registro detallado de todas las operaciones sobre el fichero, incluyendo usuario, fecha y hora, tipo de operación y resultado de la autenticación y autorización.

6.2 LSSI-CE

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE 34/2002, de 11 de julio) intenta cubrir el hueco legal que había con las empresas que prestan servicios de la sociedad de la información. La ley es de obligado cumplimiento para todas las webs que consiguen algún tipo de ingreso, bien directo (pago de cuotas, venta de productos y servicios), bien indirecto (publicidad). La primera obligación que tienen es incluir en su página información de la persona o empresa que está detrás de esa página: nombre o denominación social, dirección postal, datos de inscripción en el registro de la propiedad mercantil, etc.01 Conceptos sobre seguridad informática