Seguridad física y lógica



**Autor**

Javier Morcillo Marín

# 1 Introducción

Tanto en las organizaciones como en los domicilios particulares el uso de sistemas informáticos con acceso a Internet es generalizado por lo que preservar la información y la integridad de estos sistemas es primordial.

Hoy en día realizamos muchas gestiones a través de Internet, negocios, compras, interacción con el banco... todas estas gestiones son de carácter bastante privado y delicado por lo que hay que mantener nuestro sistema lo más seguro posible para evitar que se intercepten nuestros datos o que se infecte la red de nuestra casa u organización.

Cualquier fallo podría suponer una gran pérdida económica, material o personal o en el peor de los casos podríamos sufrir suplantación de nuestra personalidad para realizar delitos.

No obstante en términos de seguridad, no es suficiente quedarnos con las comunicaciones, este concepto, como se desarrollará en los siguientes puntos, es mucho más amplio.

# 2 Objetivos de la seguridad

En esta unidad se dará a conocer conceptos usados en los ámbitos de seguridad ampliamente dicho.

Como tal, el primer concepto que se va a definir el el de **activo** de una organización. Un **activo** de una organización (o incluso personal) es todo aquel material físico o lógico que proporciona valor a la organización, sin él, la organización perdería poder, normalmente monetario.

Según **ISO-27001** se puede definir como *“Cualquier valor cuantificable de naturaleza material o inmaterial de una organización”*.

Los objetivos principales de la seguridad son proteger los activos de una entidad, tales se pueden clasificar en:

* **La información contenida:** Uno de los elementos más importantes. Se debe evitar que los usuarios no autorizados explícitamente puedan acceder a la información ya que podrían robarla, destruirla, hacer un mal uso de ella, … Además, se debe asegurar que la información está disponible para los usuarios autorizados.
* **El software:** Es importante proteger el software que se utiliza ya que es la herramienta de trabajo con los que se construye valor.
* **La infraestructura física:** Se debe velar porque los equipos funcionen de la forma adecuada previendo medidas en caso de robo, incendio, accidentes o desastres naturales, …
* **Los usuarios:** Se deben establecer unas normas que minimicen los riesgos físicos o de datos personales de todas aquellas personas que estén relacionados con la organización o entidad, bien sean empleados o clientes.

Según entidades de estandarización:

* Según la **ISO27002:** “La seguridad de la información se puede caracterizar por la preservación de la confidencialidad, integridad y la disponibilidad”
* Según **INFOSEC Glosssary 2000**: “ Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican”.

## 

## 

# 3 Definiciones

A continuación se explican los conceptos que aparecen en las definiciones anteriores así como en los temas de seguridad en general.

* **La confidencialidad:** Hacer que la información le llegue **sólo** a las personas o entidades autorizadas. De esta manera un documento será confidencial si sólo puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada.
* **Integridad:** Capacidad de hacer que los datos no sean alterados sin el consentimiento de su autor.
* **Disponibilidad:** La información ha de ser capaz de llegar a las personas o entidades autorizadas siempre que la requieran.
* **Autenticación:** Esta característica intenta confirmar que una persona, máquina o entidad es quien dice ser, y no un impostor. Esta autenticación se puede realizar mediante algo que tienes (como una tarjeta), algo que sabes (usuarios y contraseñas) o algo que eres (biometría). Cuantos más criterios debamos cumplir, más seguro es el sistema.
* **Autorización:** Una vez autenticados, los usuarios tendrán ciertos privilegios sobre la información, tales son: acceso, lectura, escritura, ejecución y modificación.
* **Cifrado:** Mecanismo por el que se codifica un mensaje mediante una clave y/o algoritmo haciéndolo ininteligible para aquellos que no conocen la clave y/o algoritmo que lo pueda decodificar. Para todo aquel que no supere la autenticación oportuna, la información estará invisible o cifrada.
* **Accounting:** Trata de hacer el seguimiento de las acciones que hace todo usuario registrado.
* **No repudio:** Que la comunicación entre emisor y receptor queden garantizadas y que ninguno pueda negar que ha existido.
  + **No repudio en origen:** El emisor no puede negar la comunicación ya que se le envían pruebas al receptor de tal comunicación.
  + **No repudio en destino:** El receptor no puede negar la comunicación porque el emisor tiene pruebas de la recepción.
* **Vulnerabilidad:** Defecto de un sistema que puede ser usado para atacarlo. Éstas pueden ser reconocidas (con y sin parche), o no reconocidas. Es conveniente actualizar siempre nuestro software y hardware. Según **ISO-27001**, *“Factor de riesgo interno de un sistema expuesto a una amenaza, y se corresponde con su predisposición intrínseca a ser afectado o susceptible de daño”*.
* **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice. Según **ISO-27001**, *“Probabilidad de que una amenaza explote una vulnerabilidad”*.
* **Impacto:** Eficacia del daño producido ante un ataque. Según **ISO-27001**, *“Cuantificación del daño ocasionado una vez materializada la amenaza”*.
* **Desastres:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios de una organización.
* **Plan de contingencia:** Políticas de seguridad que contemplan parte de la prevención de un sistema, pero no hay que desechar la posibilidad de que, aun a pesar de estas medidas, pueda ocasionarse un desastre. Se basa en los siguientes principios:
  + Evaluación de los peligros.
  + Planificar las actuaciones para conseguir una recuperación total.
  + Hacer pruebas para evaluar su eficiencia y su eficacia.
* **Centro de proceso de datos:** CPD, es un sitio centralizado donde se procesan y/o almacenan los datos.

## 

## 

# 4 Amenazas

Se puede definir amenaza, según **ISO-27001**, como *“Factor de riesgo externo representado por un peligro latente asociado a un fenómeno natural, tecnológico o humano, pudiendo manifestarse en un sitio específico por un tiempo determinado, produciendo efectos adversos a personas o bienes”*.

Una vez que alguien decida atacarnos (aunque sea la propia naturaleza), puede elegir una de las siguientes formas:

* **Interrupción:** El ataque consigue provocar un corte en la prestación de un servicio. Un ataque puede hacer caer un servidor, o romper el ordenador que hace de servidor.
* **Interceptación:** El ataque ha conseguido capturar (copiar) información.
* **Modificación:** El ataque altera el contenido de la información.
* **Fabricación o suplantación:** El ataque consiste en engañar a un usuario haciéndole creer que el atacante es el destinatario de una petición.

Además existe una clasificación paralela:

* **Amenazas activas:** Amenazas que están siempre intentando atacar para poder producir modificación de los activos.
* **Amenazas pasivas:** Amenazas latentes como pueden ser las escuchas.

## 4.1 Técnicas de ataque

Para conseguir alguno de los puntos anteriormente dichos se pueden utilizar alguno de las siguientes técnicas

* **Ingeniería social:** Se trata de utilizar los medios humanos no informáticos para que alguien nos proporcione información o haga algo que en principio no haría. Tales medios pueden ser engaños, amenazas, ...
* **Spoofing:** Suplanta la identidad de otro dispositivo u ordenador.
* **Sniffing:** Analiza el tráfico de red para hacerse con información.
* **Conexión no autorizada:** Se busca un agujero de seguridad y se entra en el sistema.
* **Malware:** Se introducen programas malintencionados en nuestro sistema. Se pueden clasificar en los siguientes:
  + **Virus:** Intentan hacer inservible un dispositivo.
  + **Gusanos:** Van acaparando poco a poco todos los recursos de un ordenador.
  + **Troyanos:** Habilitar puertas traseras para que se puede entrar al sistema.
* **Keyloggers:** Almacenan lo que se teclea e incluso hacen capturas de pantalla para posteriormente enviárselo a alguien.
* **Phishing:** Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o página web.
* **Fuerza bruta:** Utilizar todas las combinaciones posibles de caracteres para romper una contraseña.
* **Denegación de servicio:** Denial of Service, o DoS, consiste en tumbar a un servidor o una red haciendo más peticiones de las que pueda soportar.
* **Denegación de servicio distribuida:** DDoS, Lo mismo que DoS, pero utilizando muchos ordenadores.

## 4.2 Tipos de atacantes

Los ataques anteriormente citados los puede hacer alguno de los siguientes perfiles.

* **Hackers:** Atacan sistemas con buenas intenciones.
* **Crackers:** Hacker que quiere causar daño u obtener beneficio.
* **Phreakers:** Crackers telefónicos.
* **Sniffers:** Analizan el tráfico de la red para obtener información de los paquetes transmitidos.
* **Lammers:** Se consideran Hackers pero no tienen suficientes conocimientos para ello.
* **Newbie:** Hacker novato.
* **Ciberterrorista:** Cracker que trabaja para países u organizaciones como espías o saboteadores.
* **Programadores de malware:** Crean programas dañinos para los sistemas o aplicaciones.
* **Carders:** Atacan sistemas de tarjetas de crédito.
* **Delincuente físico:** Persona común que utiliza la fuerza física o chantaje emocional.

## 

## 

# 5 Seguridad ante ataques

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad , la integridad y la disponibilidad de un sistema informático así como contrarrestar los efectos de un ataque.

Los mecanismos pueden clasificar según su función en:

* **Preventivos:** Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
* **Detectivos:** Actúan también antes de que un hecho ocurra pero su función es revelar la presencia de agentes no detectados en algún elemento del sistema.
* **Correctivos:** Actúan después de que haya ocurrido el hecho y su función es corregir las consecuencias.

Según lo que se protege se puede distinguir entre:

* **Seguridad física:** Es aquella que trata de proteger el hardware de los posibles desastres naturales (incendios, inundaciones, ...), sobrecargar eléctricas, robos…
* **Seguridad lógica:** Protege el software de los sistemas informáticos a la vez que los datos almacenados digitalmente. La seguridad lógica se encarga de controlar que el acceso al software de un sistema informático se realiza por los usuarios adecuados y de la forma correcta.

Dependiendo del momento en el que se actúa entre:

* **Seguridad activa:** Son aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema.
* **Seguridad pasiva:** Comprende el conjunto de medidas utilizadas para que una vez que se produzca el ataque o fallo intentar minimizar los daños y activar los mecanismos de recuperación.

En la siguiente tabla se muestran amenazas, prevenciones y elementos que pueden amortiguar los resultados de esos ataques de ataques.

|  |  |  |
| --- | --- | --- |
| **Técnicas** | **¿Que previene?** | **Tipo** |
| Contraseñas | Previene el acceso a recursos a usuarios no autorizados | Lógica  Activa |
| Listas de control de acceso (ACL) | Previene acceso a ficheros a usuarios no autorizados | Lógica  Activa |
| Encriptación | Evita a personas no autorizadas interpretar la información | Lógica  Activa |
| Software de seguridad | Evita virus y accesos no deseados al sistema | Lógica  Activa |
| Firmas y certificados digitales | Comprueba la procedencia, autenticidad e integridad de los mensajes | Lógica  Activa |
| Sistemas de ficheros tolerantes a fallos | Previene fallos de integridad | Lógica  Activa |
| Cuotas de disco | Previene el uso excesivo de disco por parte de algún usuario | Lógica  Activa |
| Discos redundantes | Restaurar datos que han quedado inconsistentes | Lógica  Pasiva |
| SAI | Fallos de suministro de energía durante un periodo de tiempo.  Hace de filtro ante picos de tensión. | Física  Pasiva |
| Copias de seguridad | Podemos recuperar información en caso de pérdida de datos. | Lógica  Pasiva |
| Controles biométricos y tarjetas. | Robos.  Acceso a zonas restringidas. | Física  Activa |
| Cámaras de seguridad y vigilantes. | Robos.  Acceso a zonas restringidas.  Control de visitas. | Física  Activa |
| Formación del personal. | Desastres por error.  Aplicar medidas de contingencia. |  |
| Antivirus | Infección de malware. | Lógica |
| Revisar los logs del sistema | Encontrar intentos de ataques de la red, de virus, ...  Encontrar fallos en el software y en el hardware. |  |
|  |  |  |
| **Amenaza** | **Medidas preventivas** | **Tipo** |
| Incendios | Mobiliario ignífugo.  Evitar localización peligrosa  Sistemas de extinción de incendios, detectores de humo…  Sellado de las plantas y las salas.  Uso de extintores. | Física |
| Inundaciones | Evitar plantas bajas.  Impermeabilización de paredes, techos, sellado de puertas... | Física |
| Señales electromagnéticas | Evitar lugares con radiaciones electromagnéticas  Filtros o cableado especial. La fibra óptica no es sensible a esto. | Física |
| Sobrecargas eléctricas | Estabilizadores de la señal eléctrica (normalmente los SAI lo hacen) | Física |
| Desastres naturales | Estar en contacto con los organismos que proporcionan información sobre terremotos o desastres meteorológicos.  Localización de los recursos en un sitio más seguro. | Física |
| Actos vandálicos y sabotajes. | Políticas de planes de contingencia. | Física |
| Humedad | Conseguir una humedad ambiental del 50% | Física |
| Espacio | Tener zonas de paso donde no exista el riesgo de romper nada. | Física |
| Calor | Hay que intentar tener un entorno entre 15-25º  Tener buena ventilación en los equipos.  Evitar la luz solar.  Poner refrigeración. | Física |
| Suciedad e insectos | Evitar las partículas de polvo.  Tener la zona de trabajo limpia y en orden.  No dejar comida. | Física |
| Campos magnéticos | Evitar los campos magnéticos en material sensible a ellos como monitores, antenas, ... | Física |
| Vibraciones | Evitar crear vibraciones que deterioren el material. | Física |
| Electricidad. | No tener suelos que acumulen electricidad estática.  Tener tomas de tierra. | Física |
| Robo de datos | Cifrado.  Contraseñas  Sistemas biométricos | Lógica |
|  |  |  |
| **Amenaza** | **Medidas preventivas** | **Tipo** |
| Pérdida de información por malfuncionamiento | Copia de seguridad (distintas ubicaciones)  Sistemas tolerantes a fallos  Discos redundantes | Lógica |
| Pérdida de integridad de la información | Programas de chequeo del equipo.  Firma digital  Comando sfc (System file checker) | Lógica |
| Ataques desde la red | Firewall  Programas de monitorización  Proxys | Lógica |
| Modificaciones no autorizadas | Contraseñas  Listas de control de acceso  Cifrar documentos | Lógica |

## 5.1 Recomendaciones de seguridad

Como se ha visto anteriormente existen numerosas amenazas para las cuales se pueden establecer mecanismos de seguridad que minimicen o anulen los daños e incluso evitar que se lleguen a intentar producir.

Algunas de las recomendaciones que se pueden aplicar, pueden encontrarse entre las siguientes, a su vez, algunas ya se han comentado en los puntos anteriores:

* Mecanismos software o lógicos
  + Redactar y revisar planes de actuación ante catástrofes.
  + No instalar nada que no sea estrictamente necesario.
  + Revisar las configuraciones del software.
  + Activar las actualizaciones automáticas.
  + Gestionar y revisar los logs de las aplicaciones y el sistema operativo.
  + Revisar la lista de equipos conectados.
  + Revisar la lista de usuarios autorizados.
  + Avisos por SMS o eMail para informarnos de ataques.
  + Usar cortafuegos, antivirus y antispam.
  + Encriptar la información, el sistema de archivos y las comunicaciones mediante técnicas de cifrado seguras.
  + Usar certificados digitales y firmas digitales.
  + Uso de contraseñas.
  + Mantener un listado de usuarios activos y sus permisos a poder ser centralizada.
  + Tener listas de control de acceso (ACL)
  + No instalar nada innecesario
  + Actualizar parches de seguridad
  + Hacer copias de seguridad
  + **Usar contraseñas seguras**
    - Evitando: nombres, fechas de nacimiento, nombre de mascotas, …
    - Que al menos tenga 8 caracteres
    - En wifi, al menos 16 caracteres en WPA2.
    - Que tengan mayúsculas y minúsculas.
    - Que tengan caracteres que no sean ni letras ni números.
* Mecanismos hardware o físicos
  + Usar SAIs, extintores, cámaras de seguridad, …
  + Hacer controles de acceso físico al sistema como pueden ser las tarjetas de identificación
  + Control de la temperatura y la humedad de la habitación donde se encuentran los ordenadores.
* Mecanismos comunes
  + Localizar los activos que hay que proteger y revisar las políticas de seguridad.
  + Hacer planes de contingencia eficaces y eficientes.
  + Formación a los usuarios.
  + Hacer auditorías externas.

# 

# 

# 6 Ejercicios

# Ve al apartado del tema donde se ofrecen una serie de definiciones como integridad, confidencialidad, no repudio, …

# Ponte de acuerdo con un compañero/a de clase.

# Uno de los/las dos deberá leer las definiciones pares y el otro las impares.

# Una vez hecho esto, cada uno deberá explicarle a la otra persona las definiciones que ha leído y tendrás que:

# Escribir lo que has entendido en el cuaderno de clase.

# Explicar una de ellas en clase, para ver que efectivamente lo has entendido.

1. Piensa en los perfiles de atacantes que hay en el tema. ¿Hay alguien en tu clase que creas que el día de mañana pueda responder a un de ellos? Explica por qué, aunque no pongas el nombre propio.

NO LO CREO, NO VEO A NADIE DE ESTA CLASE DEDICÁNDOSE AL HACKEO.

1. De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado (activa, pasiva, lógica y física)
   1. Ventilador de un equipo informático. FÍSICA Y ACTIVA
   2. Detector de incendio. FÍSICA Y ACTIVA
   3. Detector de movimientos. FÍSICA Y ACTIVA
   4. Cámara de seguridad. FÍSICA Y ACTIVA
   5. Cortafuegos. LÓGICA Y ACTIVA
   6. SAI. FÍSICA ACTIVA Y PASIVA
   7. Control de acceso mediante el iris del ojo. FÍSICA Y ACTIVA
   8. Contraseña para acceder a un equipo. LÓGICA Y ACTIVA
   9. Control de acceso a un edificio. FÍSICA Y ACTIVA
2. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
   1. Terremoto.FÍSICA
   2. Subida de tensión.FÍSICA
   3. Virus informático.LÓGICA
   4. Hacker.LÓGICA
   5. Incendio fortuito.FÍSICA
   6. Borrado de información importante.LÓGICO
3. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.
   1. Antivirus. ACTIVA Y PASIVA
   2. Uso de contraseñas. ACTIVA
   3. Copias de seguridad. PASIVA
   4. Climatizadores. ACTIVA
   5. Uso de redundancia en discos. PASIVA
   6. Cámaras de seguridad. PASIVA
   7. Cortafuegos. ACTIVA
4. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
   1. mesa NO, ES CORTA Y SOLAMENTE CONTIENE LETRAS
   2. caseta NO, ES CORTA Y SOLAMENTE CONTIENE LETRAS
   3. c8m4r2nes SÍ, ES LARGA Y CONTIENE NÚMERO ADEMÁS DE LETRAS
   4. tu primer apellido NO, PORQUÉ TU APELLIDO SOLAMENTE CONTIENE LETRAS Y NORMALMENTE SON CORTOS
   5. pr0mer1s& SÍ, CONTIENE NÚMEROS, LETRAS Y SÍMBOLOS ESPECIALES.
   6. tu nombre NO, ES CORTO Y SOLAMENTE CONTIENE LETRAS
5. Ordena de mayor a menor seguridad los siguientes formatos de claves.
   1. Claves con sólo números.1
   2. Claves con números, letras mayúsculas y letras minúsculas.4
   3. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.5
   4. Claves con números y letras minúsculas.3
   5. Claves con sólo letras minúsculas.2

# 7 Prácticas

1. En el cuaderno de clase enumera 5 casos en los que alguien quisiera utilizar algún método que violara la seguridad, porque quiere vulnerar la seguridad y con qué fin.

-Un exempleado con motivo de venganza

-Una empresa para empeorar la posición de otra.

-Alguien para robar

-Alguien para espiar.

-Cualquiera por diversión.

1. Busca qué es una ACL, entiéndelo, y explícalo en clase.

ES un sistema que permite y garantiza el acceso al igual que lo deniega a x usuarios a realizar x operaciones

1. Busca qué es sfc, entiéndelo, y explícalo en clase.

Es una facilidad que ofrece Windows a sus usuarios y les permite escanear y restaurar archivos corruptos

1. Describe los medios de seguridad física y lógica que hay en el aula.

Físico- Extintor, estufa, ventilador y seguridad del cableado general.

Lógico- SO Ubuntu

1. Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.

Activa: Antivirus, contraseñas.

Pasivas: Copias de seguridad

1. Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.

No tengo protección ante cortes de luz, subidas y bajadas de tensión, incendios y demás desastres naturales

1. Busca en Internet las claves más comúnmente usadas.

-123456

-password

-qwerty

-abc123

1. Decides montar una empresa en Internet que se va a dedicar a ofrecer un disco duro on-line. Necesitas de cada usuario: nombre, teléfono y dirección de correo electrónico. ¿En qué afectar estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenamos esta información?

En qué deberás proteger la privacidad de tus usuarios así como su información.

Encriptar dicha información y poner autenticadores.

1. Busca en Internet un protocolo de actuación ante un desastre natural, cita las cosas que veas interesantes (que tipo de personas interviene), pues las vas a explicar en clase, y añade a ese protocolo las medidas que consideres para no perder la información de la organización.

En caso de seísmo

Si fuese aquí en el centro, actuarían tanto el profesorado como el alumnado incluyendo, claro está a los servicios de emergencia.

En primer lugar debería haber un sistema de prevención de accidentes, para prevenir males mayores.

-Buscar un lugar seguro bajo una mesa o un objeto sólido resistente.

-Colocarse en una zona abierta.

-NO utilizar ascensores.

# 

# 8 Bibliografía

* Costas Santos, Jesús Seguridad informática Editorial RA-MA
* García-Cervigón Hurtado, Alfonso et al. Seguridad informática Editorial Paraninfo
* Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill
* Aplicación de la ley de protección de datos: <https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/medidas_seguridad/index-ides-idphp.php>