SEGURIDAD INFORMÁTICA

SiStemaS microinformáticoS y redeS

Ilerna

ILERNA, centro autorizado con código 25002775 (Lleida), 28077294 (Madrid) y 41023090 (Sevilla)

www.ilerna.es

Maquetado e impreso por Ilerna Online S.L.

Impreso en España - Printed in Spain

terceros en esta obra y se excusa con antelación por posibles errores u omisiones y queda a disposición de corregirlos en posteriores ediciones.

2.ª edición: abril 2021

ÍNDICE

Seguridad informática

1

SEGURIDAD FÍSICA Y LÓGICA

En función de las necesidades y aspectos a salvaguardar, disponemos de varios tipos de seguridad.

En este punto detallaremos los mecanismos existentes para realizar acciones de **seguridad** para el **equipo físico** ante:

- cualquier catástrofe meteorológica.
- o robo del equipo.

y las opciones de seguridad disponibles para la **parte lógica** de nuestro equipo, es decir, los datos que tenemos almacenados.

Gestionar de forma permanente la seguridad física es el comienzo para integrar la protección como una función primordial dentro de cualquier sistema.

El control del ambiente y **el acceso físico** permite:

disminuir los siniestros

y realizar unas tareas de mantenimiento de una forma más liviana, ya que se pondrán en marcha las medidas de protección preventiva que tendremos instaladas.

Asimismo, debemos conocer en todo momento el estado de nuestro sistema para tomar decisiones sobre las medidas preventivas que se están llevando a cabo.

1.1. UBICACIÓN FÍSICA Y CONDICIONES AMBIENTALES DE LOS EQUIPOS SERVIDORES

Ubicación física

A la hora de establecer la seguridad de un equipo o servidor, el primer paso es determinar en qué **lugar vamos a instalarlo**, decisión fundamental para:

- El mantenimiento.

Seguridad física I

youtu.be/O-57v9jL8HU

- Y la protección de nuestro sistema

Consiste en establecer barreras físicas y procedimientos de control para una protección total del equipo y de la información que contiene.

Para decidir la ubicación física del equipo hay que tener presente una serie de :, ya que habrá que valorar factores como:

El edificio donde se instala el equipo.

- El tamaño y ubicación del mismo,
- La ventilación,
- La iluminación,
- El espacio del que se dispone
- El tipo de acceso de los dispositivos y del personal.

También será necesario observar

- las características de las instalaciones de suministro eléctrico
- o de acondicionamiento térmico, entre otras cosas.

Otro de los aspectos para tener en cuenta es la acústica, pues habrá que controlar **los niveles de ruido** ya que, por lo general, aparte de los **EQUIPOS INFORMÁTICOS** también habrá

EQUIPOS DE VENTILACIÓN,

como –> aires acondicionados.

Si superamos los niveles normales de ruido entre todos esos elementos, habrá que amortiguarlo mediante alguna reparación en la sala, para que no ocasionen molestias.

Por otra parte, también hay que evaluar la seguridad física del edificio, que debe contemplar:

- el plan de emergencia contra incendios.
- y la protección contra inundaciones.
- y otros factores de índole natural susceptibles de dañar de algún modo la instalación.

Condiciones ambientales

Además de lo mencionado anteriormente, también hay que tener en mente otros factores como la **localización** y las **condiciones ambientales** del entorno en el que instalaremos los equipos.

Lo principal es valorar factores naturales como el frío, el calor, la humedad, las inundaciones, los incendios o los terremotos.

Se aconseja que la humedad relativa sea del 50%, pues el exceso de esta provoca que los componentes se corrosionen y su escasez genera electricidad estática.

Por otra parte, la temperatura idónea para los dispositivos eléctricos es de 15 a 25 ^{o}C.

➔ Si la temperatura ambiental no está dentro de este rango, será necesario utilizar aparatos de refrigeración o calefacción para conseguir la temperatura adecuada.

En cuanto a los terremotos, las vibraciones y los golpes, estos pueden provocar averías, especialmente en los discos duros de los equipos informáticos.

1.2. PROTECCIÓN FÍSICA DE LOS SISTEMAS INFORMÁTICOS

Si se produce un robo, se pueden recuperar las materias sustraídas, pero lo más importante es tener implementadas unas medidas de seguridad para que estos hechos no acontezcan.

Cuando este tipo de incidentes tienen lugar en una empresa,

suelen resultar mucho más graves, pues pueden robar datos mucho más sensibles e irremplazables.

Además, en otros casos también pueden afectar al patrimonio, al mobiliario o a los ordenadores, lo que sí se podría reemplazar más fácilmente que lo anterior.

Para proteger un sistema informático y garantizar su seguridad física se emplean **barreras físicas** y **procedimientos de control frente a amenazas físicas** al hardware.

8

CONCEPTO

La seguridad física es el conjunto de medidas **que se realizan para** prevenir **y detectar daños físicos en los sistemas informáticos y así proteger los datos que se encuentran almacenados en ellos.**

La seguridad física trata de proteger el hardware ante posibles daños y desastres naturales como incendios, inundaciones, golpes, robos, sobrecargas eléctricas, etcétera.

Estos riesgos externos a los que están sujetos los equipos informáticos pueden prevenirse de la siguiente manera:

- **FENÓMENOS NATURALES**: incendios, inundaciones, sobrecargas eléctricas, etcétera.

Las medidas preventivas en estos casos se basan, principalmente, en una ubicación adecuada de los equipos, dotada de las oportunas medidas de protección.

- **RIESGOS HUMANOS**: actos involuntarios como golpes o arañazos, actos vandálicos y sabotajes.

-

Las medidas preventivas a seguir serían:

- El control de los accesos a los recintos en los que están los equipos,
- La elaboración de perfiles psicológicos de empleados con acceso a datos confidenciales,
- La formación en materia de seguridad a los usuarios que manipulen los equipos, etcétera.
-

En este apartado nos centraremos en las medidas de protección de los **equipos informáticos** y dejaremos las medidas de seguridad de los servidores para próximos puntos, ya que estos suelen localizarse en salas especiales.

Entorno físico

Uno de los apartados más relevantes a la hora de diseñar las medidas de seguridad es el emplazamiento del equipo en el lugar de trabajo.

De esta forma, podemos definir las condiciones físicas que determinan este tipo de riesgos, junto con su medida preventiva.

- **ESPACIO**: los equipos informáticos, al ser máquinas eléctricas, necesitan disipar el calor que producen, por lo que necesitan localizarse en lugares con buena ventilación.

- Igualmente, no debemos obstaculizar con algún objeto la salida de los ventiladores del equipo.

- **Luz solar**: debemos evitar la luz solar directa, ya que puede producir un sobrecalentamiento.
  - ➔ La instalación de persianas o cortinas en la habitación puede ser una buena solución.

- **Temperatura**: hay que tener muy presente todo lo relacionado con la temperatura. Lo hemos comprobado en los puntos anteriores, donde se ha hablado del sobrecalentamiento y de la humedad (se aconseja tenerlo a un 50% para su buen rendimiento).

- **Campos magnéticos**, **vibraciones** y **el tipo de suelo**: también serán factores que valorar.

Instalaciones

Además de las condiciones ambientales, existen otros factores que entrañan riesgos para el equipo informático.

1 - En primer lugar, debemos comprobar que hemos ubicado el dispositivo cerca de una **instalación eléctrica adecuada**, ya que los equipos informáticos funcionan gracias a esta fuente de energía.

Esta instalación puede tener enchufes con toma de tierra o ser un sistema de alimentación ininterrumpida, con aparatos para estabilizar la corriente en la red. Estas modificaciones se toman como medida preventiva.

---

2 - En segundo lugar, nos ocuparemos de la **instalación de la red de equipos**.

Para ello, debemos elegir un tipo de cable adecuado y controlar el acceso de los distintos clientes mediante claves.

3 - Por último, debemos gestionar la **prevención contra incendios** mediante sistemas de prevención y protección.

A) La prevención pasa por la instalación de detectores de humo y el mantenimiento higiénico de la sala,

B) Mientras que la protección comprende la adecuada señalización para que, si se produce un incendio, los trabajadores puedan encontrar fácilmente cual el camino de la evacuación.

- ➔ La instalación de extintores sería otro ejemplo de medida de protección.

a. SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

Es recomendable un **suministro eléctrico** propio del **CPD** (centro de procesamiento de datos),

con independencia respecto al resto de la instalación

y que cuente con elementos de protección y seguridad específicos, como, por ejemplo,

sistemas de alimentación ininterrumpida. SAI

De este modo, conseguiremos que:

- los equipos no estén sujetos a fluctuaciones,
- picos de la red,
- sobrevoltajes
- o ruidos electrónicos que puedan hacerles sufrir.

Este **suministro propio** se puede conseguir a través de:

- equipos electrógenos,
- baterías,
- etcétera.

Un **SAI** o **sistema de alimentación ininterrumpida** es un dispositivo electrónico que protege los equipos en situaciones de picos o caídas de tensión.

Así, la **estabilidad es mayor incluso si se producen cambios del suministro eléctrico** y que al usar una **fuente de alimentación auxiliar** cuando hay un corte de luz.

Estos sistemas fueron creados para proteger el trabajo que se estuviera haciendo en caso de apagón.

Nació con la idea de que, ante un corte del suministro eléctrico, el usuario tuviera tiempo suficiente para guardar la información y apagar bien los equipos.

Más adelante, se le añadió más capacidad para poder seguir trabajando durante un determinado periodo de tiempo, sin necesidad de disponer de suministro.

b. APLICACIÓN DE LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

En este apartado nos centraremos en las características y **tipos** de SAI que existen en el mercado, los cuales dependen del funcionamiento que tienen:

1 ***Offline*** **pasivo**: es el tipo más habitual para proteger los equipos.

- Activa la alimentación desde las baterías de forma automática al detectar un fallo en el suministro eléctrico.

Este corte eléctrico que se produce desde que se detecta el fallo hasta que se activa el SAI es tan pequeño que lo normal es que los equipos no detecten la interrupción de energía.

2 ***Offline*** **interactivos**: estos se encuentran conectados a la corriente, la cual alimenta al ordenador de manera continua, aunque no haya problemas en el suministro eléctrico, y a la vez carga la batería.

V La ventaja de este dispositivo es que ofrece una tensión de alimentación constante, pues filtra los picos de la señal eléctrica susceptibles de dañar el ordenador.

Normalmente, suelen usarse para proteger pequeños servidores o equipos de pequeñas empresas.

3 **SAI** ***online***: se colocan entre la red eléctrica y los equipos.

Están siempre enchufados a la corriente eléctrica, a la vez que proporcionan energía a los dispositivos que protegen. Aunque son los dispositivos más caros y de más calidad, tienen el inconveniente de que deterioran la batería por estar en continuo contacto con la corriente eléctrica.

Las partes que forman este dispositivo estabilizador eléctrico las detallamos a continuación:

a. **BATERÍA**: es uno de los elementos fundamentales, ya que es lo que se tiene que cargar para que actúe cuando haya apagones en el suministro.

b. **FILTRO**: es la parte del dispositivo encargado de limpiar la señal de entrada.

c. **CONVERSOR** (**o transformador**): convierte los voltajes para adaptarlos al dispositivo.

d. **INVERSOR**: transforma la corriente continua en corriente alterna.

e. **CONMUTADOR: en caso de necesitarlo, elige entre la energía de la batería o del suministro.**

El uso de un dispositivo que regule la corriente eléctrica hace que el sistema sea mucho más estable y presente una autonomía para poder seguir trabajando en caso de fallo eléctrico. De esta forma, el usuario del equipo tiene tiempo para terminar la tarea que estaba realizando y apagar el equipo como es debido.

POLÍTICAS DE SEGURIDAD BASADAS EN LISTAS DE CONTROL DE ACCESO

Empezaremos este apartado con el concepto de seguridad lógica.

CONCEPTO

La seguridad lógica es la agrupación de medidas que se toman para proteger las aplicaciones y los datos y restringir el acceso solo a personas autorizadas.

Las políticas de seguridad que adopte cualquier empresa serán las normas que deban seguir todos los usuarios de la empresa o red.

Estas normas marcan las pautas de utilización del sistema y los protocolos de actuación a seguir en su operativa.

Entre las políticas de seguridad podemos encontrar:

- las del mantenimiento de equipos,
- el uso de los recursos de la red,
- la adquisición del software,
- la privacidad
- y la autentificación del usuario.

Para poder implementarlas, debemos tomar algunas medidas preventivas básicas de seguridad como la utilización de firmas digitales para la autentificación del usuario ante cualquier documentación personal de una entidad pública.

Otra de las medidas es la **lista del control de acceso**, donde se controla a los usuarios

a los que se les

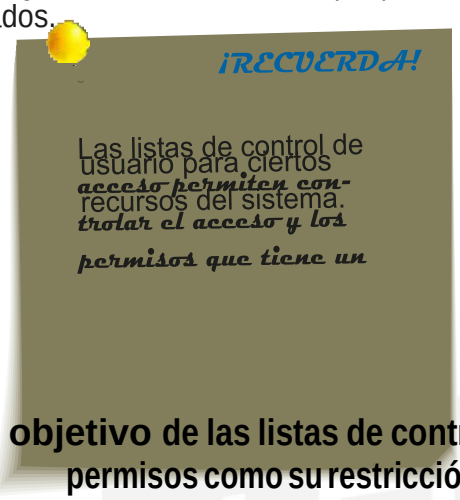
V permite entrar y…

V realizar determinadas.

La **encriptación** de datos también se suele utilizar, sobre todo para la transmisión de los datos desde un emisor a un receptor.

En este apartado, nos centraremos en las listas de control de acceso, también llamado **ACL** (como sus siglas en inglés).

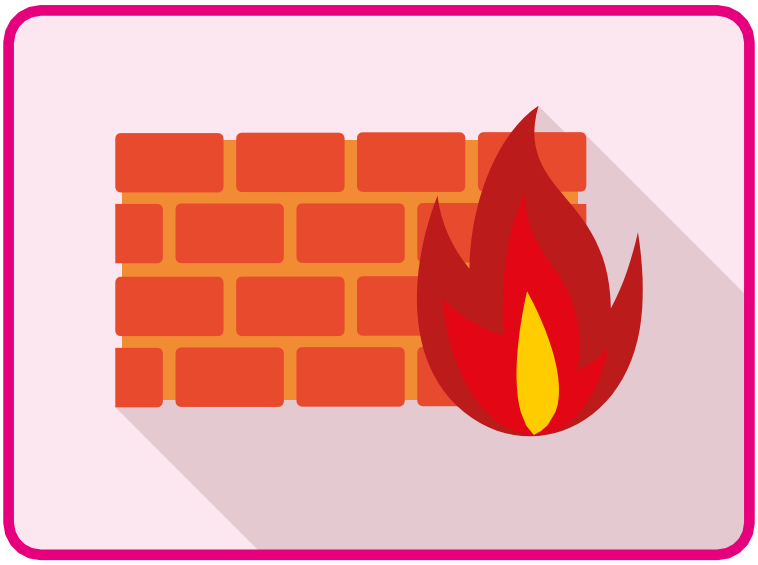
Como ya hemos mencionado anteriormente, tiene como objetivo regular el acceso al sistema por parte de usuarios no autorizados.



El objetivo de las listas de control de acceso es tanto la concesión de acceso y permisos como su restricción.

XEstas restricciones se realizan a nivel de red a través del suministro de datos que se transmiten por la misma, a nivel del sistema operativo.

- **Cada aplicación y el propio sistema operativo disponen de distintos mecanismos de seguridad que los controlan.**



- A nivel de red, disponemos de elementos como las direcciones IP o direcciones MAC, las cuales ayudan a llevar a cabo los mecanismos de control mediante el *firewall*.

Otra herramienta muy utilizada para elementos masivos es el *proxy*,

el cual controla…

…el tránsito de usuarios que entran y salen de internet en nuestra red.

Por último, el **servidor DNS y el de correo** también tienen implementados mecanismos de seguridad.

Un ejemplo muy común y que todos hemos visto es el elemento del que dispone nuestro gestor de correo electrónico para bloquear los correos *spam*.

El hecho de trabajar con **listas de control de acceso** trae una serie de **ventajas** que detallamos a continuación:

Limita el tráfico de datos: el **ACL** posibilita la mejora del rendimiento de la red, limitando el tráfico de datos en la web (como las descargas de música o videos). De esta forma, el usuario no va a poder realizar esas actividades, ya que son archivos muy pesados que pueden colapsar el tráfico de datos.

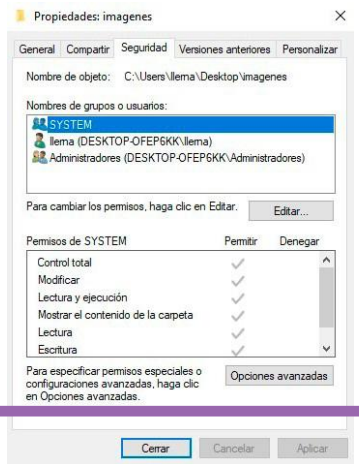
- **Concede** o **restringe** permisos y roles: en las ACL es donde se guardan los permisos o roles de los distintos usuarios a los que se le permite la entrada al sistema.

- Controla la ejecución de aplicaciones que pueden contener virus.

Las listas de control de acceso en el sistema operativo **Windows** están situadas en las **opciones de compartir los recursos**, donde se pueden distinguir dos tipos de privilegios:

- Los **permisos**: o la forma en la que podemos acceder en función del archivo.

- Los **derechos**: que establecen las acciones que están permitidas.



En el caso del sistema operativo **Linux**, existen algunas diferencias con respecto a Windows, ya que en este hay tres grupos bien diferenciados:

el propietario, grupo de usuarios y otros tipos de usuarios.

En Linux, todos los usuarios pertenecen al grupo principal.

Al **administrador** del sistema se le denomina ***root***

y, por tanto, tiene concedidos todos los **permisos.**

Es aconsejable utilizar este usuario solo en las operaciones importantes que requieran una **modificación del sistema**, como:

el acceso a la configuración del sistema operativo

o la instalación de una aplicación.

Los **permisos** en Linux se aplican a *Recurso* y pueden ser de **tres tipos(3)**,

en función de las restricciones que deseamos aplicar al recurso para algunos usuarios:

Lectura (**r**) en el que el usuario solo podrá visualizar el fichero.

Escritura (**w**) en el que el usuario puede editar el fichero y modificarlo.

Ejecución (**x**) en el que el fichero se podrá ejecutar.

Los permisos en este sistema operativo se trabajan con el comando ***chmod***, seguido de la notación ***UGO*** (propietario, grupos, otros)

y después de los **permisos** a conceder o restringir

También podemos utilizar la notación numérica en base **OCTAL**.

Hay ocasiones en las que los **permisos** no son suficientes para establecer restricciones a los usuarios sobre los recursos compartidos y, por tanto, utilizaremos las **ACL**.

Si están habilitadas, debemos activarlas con el comando *acl* al final de la correspondiente línea de partición; en caso de que no lo estén, hay que descargar el **paquete**.

Una **lista de control de acceso** se compone de entradas en las cuales se especifican los permisos a los accesos a un determinado recurso. Las entradas se dividen en: categoría, identificador y cadenas de **permisos**.

Tema 1. Seguridad física y lógica

Cuando el sistema está implantado en una organización muy grande,
➔ con departamentos en varias sedes

, es normal que trabajen con pocas aplicaciones comunes y muchas aplicaciones individuales.

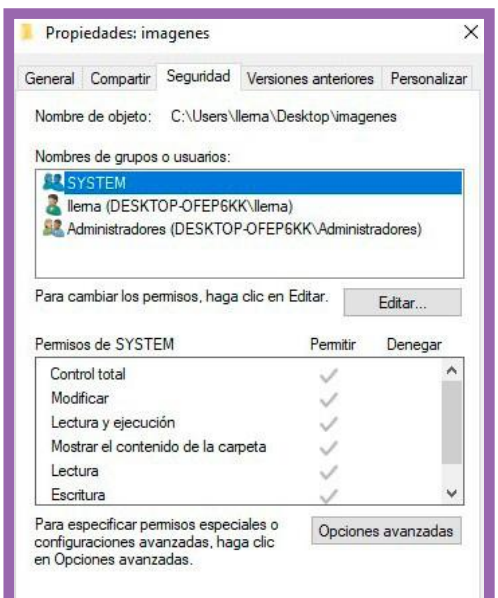
Lo que se pretende en este caso es que…
el usuario pueda acceder a todas las aplicaciones
➔ con la misma credencial,
- lo que se denomina **identidad federada**.

Además, dispone de su **versión web**, como la anterior, y recibe el nombre de **OpenId** para realizar
la gestión de las credenciales de los usuarios
desde internet.

Las listas de control de acceso en el sistema operativo **Windows** están situadas en las **opciones de compartir los recursos**, donde se pueden distinguir dos tipos de privilegios:

- Los **permisos**: o la forma en la que podemos acceder en función del archivo.

- Los **derechos**: que establecen las acciones que están permitidas.



En el caso del sistema operativo Linux, existen algunas diferencias con respecto a Windows, ya que en este hay tres grupos bien diferenciados**:**

el propietario, grupo de usuarios y otros tipos de usuarios.

En Linux, **todos los usuarios pertenecen al grupo principal**.

Al usuario administrador del sistema se le denomina *root* y, por tanto, tiene concedidos todos los permisos. Es aconsejable utilizar este usuario solo en las operaciones importantes que requieran una modificación del sistema, como el acceso a la configuración del sistema operativo o la instalación de una aplicación.

Los permisos en Linux se aplican a *Recursos* y pueden ser de **(3) tres tipos**, en función de las restricciones que deseamos aplicar al recurso para algunos usuarios:

- **Lectura** (**r**) en el que el usuario solo podrá visualizar el fichero.

- **Escritura** (**w**) en el que el usuario puede editar el fichero y modificarlo.

- **Ejecución** (**x**) en el que el fichero se podrá ejecutar.

Los permisos en este sistema operativo se trabajan con el comando ***chmod***, seguido de la notación ***UGO*** (propietario, grupos, otros) y después de los permisos a conceder o restringir. **También podemos utilizar la notación numérica** en base octal.

Hay ocasiones en las que los permisos no son suficientes para establecer restricciones a los usuarios sobre los recursos compartidos y, por tanto, utilizaremos las **ACL**. Si están habiltadas, debemos activarlas con el comando ***acl*** al final de la correspondiente línea de partición; en caso de que no lo estén, hay que descargar el paquete.

Una lista de control de acceso se compone de entradas en las cuales se especifican los permisos a los accesos a un determinado recurso.

Las entradas se dividen en:

categoría, identificador y cadenas de permisos.

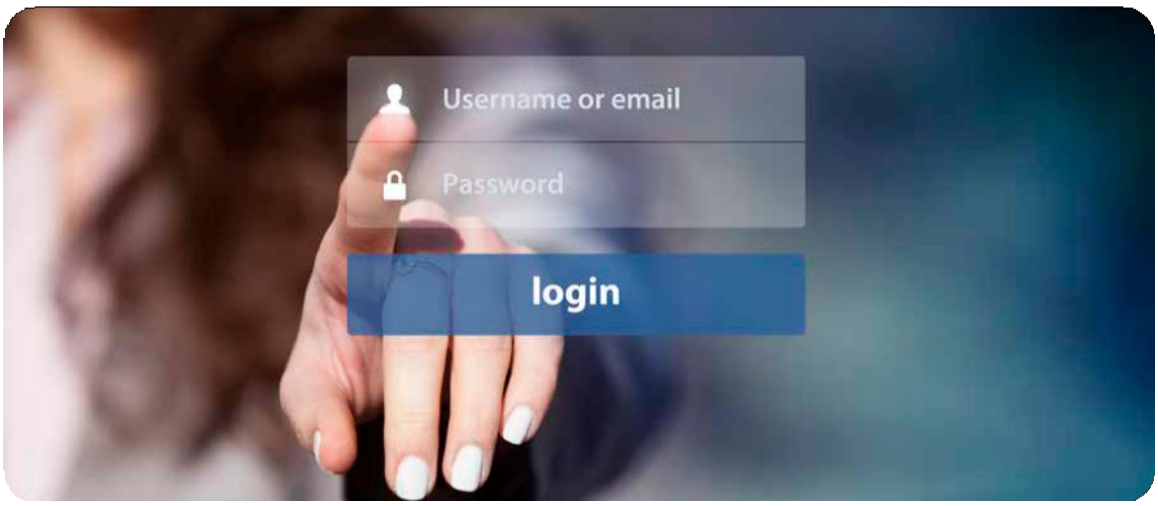
c. políticas de contraseñas; sistemas biométricos

Política de contraseña

El control de acceso al usuario en un sistema informático es una de las medidas más básicas que podemos implementar

La autentificación de los usuarios se realiza introduciendo un nombre y una contraseña.

Las credenciales de cada uno se forman a partir de un identificador y una clave, las cuales permitirán comprobar su identidad y autenticidad.



Como es lógico pensar, la seguridad del sistema va a estar relacionada con la buena elección de la contraseña y con su confidencialidad.

Por este motivo, las **empresas normalmente tienen definidas políticas de contraseñas** en las que se establecen, entre otras, algunas condiciones para crearlas (como, por ejemplo, su longitud mínima, su formato o el tiempo de validez).

A continuación, mostramos algunas **recomendaciones** para confeccionar una **buena contraseña**:

✗ **No deben estar formadas por palabras que aparezcan en el diccionario**: ni en español, inglés ni en ningún otro idioma, pues cualquier programa de fuerza bruta podría descubrir- la sin dificultad.

✗ **No deben usarse solo letras mayúsculas, minúsculas o números**: porque las combinaciones posibles se verían muy reducidas. Algunos ejemplos rechazables son *ANA*, *avestruz*, *abcdef* o *20014*.

✗ **No debemos utilizar información personal**: como el nombre de miembros de nuestra familia, la fecha de nacimiento o el número de teléfono, pues cualquiera de nuestro entorno podría averiguarla. Algunos ejemplos son: *cp28007* o *06/06/1965*. Este es un fallo muy común en las preguntas que realizan ciertas páginas (correos electrónicos) al no recordar la contraseña.

✗ **No debemos invertir palabras reconocibles**: como *atatap* o *zurtseva*. Hay programas creados para este fin que podrían descubrirlo rápidamente.

✗ **No debemos escribir la contraseña en ningún sitio**: ni en papel ni en documentos electrónicos sin encriptar.

Tampoco hay que mencionarlo por teléfono o correo electrónico, ya que estos medios de comunicación se interceptan fácilmente y existen aplicaciones que pueden desencriptar las contraseñas.

✓ **Debemos limitar el número de intentos fallidos**: si excede el número máximo de intentos permitidos, el usuario quedará bloqueado y deberá contactar con el técnico de seguridad. Esto ocurre, por ejemplo, en los cajeros automáticos: si te equivocas tres veces al introducir el pin, el cajero no te devuelve la tarjeta. De esta forma, se evita que se puedan seguir in- tentando meter la clave indefinidamente hasta que finalmente la averigüen.

✓ **Debemos cambiar las contraseñas de acceso dadas por defecto**: tanto las de los fabricantes de *routers* como las de otros periféricos que nos permiten el acceso a la red.

✗ **No debemos utilizar la misma contraseña en las distintas máquinas o sistemas**: pues, si la descubren, los demás equipos a los que tenemos acceso también serían vulnerables.

Las contraseñas deben caducar y exigir que se cambien cada cierto tiempo, como mínimo una vez al año.

✗ **No debemos** permitir que las aplicaciones recuerden las contraseñas.

✗ **No debemos** repetir los mismos caracteres en la misma contraseña.

PARA + INFO

Las contraseñas tienen que ser cadenas de caracteres compuestas por letras mayúsculas, minúsculas, números y caracteres especiales sin lógica aparente. Su longitud debe ser mayor de ocho caracteres, pero se recomienda que sobrepase los quince.

Algunos consejos para poder recordar la contraseña (pues ya hemos visto que no se recomienda escribirla en ningún sitio) serían

Elegir palabras que carezcan de sentido (pero pronunciables)

o las iniciales de una frase que seamos capaces de recordar por pertenecer a una canción que nos gusta o a algún recuerdo, como, por ejemplo: "Nací el 6 de junio del 65 en Madrid, cerca de las 6 de la madrugada", *Ne6djd6eMcdl6dlm*; para complicarla, se puede incluir algún símbolo especial en una posición que seamos capaces de recordar.

Si se siguen todas estas recomendaciones, probablemente cualquier intruso que intente descifrar la clave de acceso utilizando programas de fuerza bruta, como *John the Ripper* o similares, desista del intento al tener que perder mucho tiempo.

Es importante recordar que una mala elección o mala protección de la contraseña puede significar un agujero en la seguridad del sistema.

Para los que no tienen mucha imaginación para crear claves, existen muchos programas para generar contraseñas con las características que se quieran establecer, como *Max Passworo* y *Password Generator*.

Sistemas biométricos

Los sistemas biométricos se usan para **autentificar** a los usuarios mediante sus rasgos físicos o conductas,

es decir, **características inalterables** como:

- las huellas digitales,
- los rasgos faciales
- o el iris del ojo.

Actualmente, estos sistemas son cada vez más populares.

Por ejemplo, en Disney World, los clientes que tienen una entrada de varios días se identifican empleando este tipo de sistemas, para evitar que un grupo de amigos o familiares saque este tipo de entradas, disfrutando del descuento, para después acceder al parque por grupitos en distintos días.

El funcionamiento del **sistema biométrico** está compuesto por

(2) **dos módulos**:

---

1. el de **inscripción**
2. y el de **identificación**.

– El módulo de inscripción se encarga de:

- *leer* y *extraer* la característica identificativa del usuario mediante sensores,
- y después almacena el patrón en una base de datos.

La función del módulo de identificación es *leer* y *extraer* la seguido de la notación ***UGO*** (propietario, grupos, otros)

Característica que reconoce al usuario.

El patrón se compara con los que están almacenados en la base de datos y se devuelve la respuesta sobre la identidad del usuario.

No obstante, requiere una instalación costosa, tanto en hardware como en software, ya que viene implementado con algoritmos de reconocimiento que permiten su tratamiento.

MECANISMOS DE SEGURIDAD DE ACCESO AL SISTEMA

La seguridad del sistema es uno de los factores más importantes en un equipo.

Debemos planificar una partida presupuestaria considerable para su puesta en marcha, ya que existen distintos mecanismos que nos ayudan a gestionar el control de acceso de los usuarios al sistema,

tanto al recinto de las instalaciones

como al propio equipo.

Ya nos hemos ocupado en apartados anteriores del nivel de seguridad en el acceso de software, hablando de las credenciales y de las medidas a adoptar a la hora de crear una contraseña. En este apartado, nos centraremos en

los **mecanismos físicos** para reconocer a los usuarios cuando deseen acceder al sistema.

Se consideran **accesos** a todas aquellas aberturas o espacios de comunicación con el exterior. No solo puertas y ventanas (lo que serían accesos principales, secundarios y aperturas explícitas), sino también:

- los conductos de refrigeración y calefacción,
- las salidas para mascotas,
- los garajes y los trasteros más desprotegidos estructuralmente, pero con acceso directo a la instalación.

Para empezar con el proceso de la instalación del mecanismo, debemos tener un plano del habitáculo con cada uno de estos accesos, los cuales representan, en mayor o menor medida, un punto débil para la seguridad.

En este caso, solo nos centraremos en los accesos principales.

El acceso principal de una instalación es la **puerta de entrada**, por lo que debe ser de tanta calidad como el tipo de información que deseamos guardar.

Es importante instalar una puerta lo suficientemente segura como para mantener el acceso controlado ante personas no autorizadas, aunque es aconsejable que estas puertas vayan acompañadas por dispositivos electrónicos, para aumentar la seguridad.

Dentro de los mecanismos de seguridad podemos diferenciar entre

a) los **dispositivos por teclado** (aquellos que requieren utilizar un teclado para introducir la contraseña)

b) y los **dispositivos por tarjeta** (aquellos que registran las credenciales almacenadas en una tarjeta identificativa).

Este último se compone de un lector de tarjeta, pero en ningún momento controla al individuo que la porta. Además, presenta el inconveniente de que, en caso de sustracción, nos llevaría a un proceso complicado la duplicación de dicha tarjeta, mientras que con el dispositivo por teclado no tendríamos ese problema.

Como ya hemos mencionado anteriormente, están también los **dispositivos biométricos**. Pueden instalarse en el acceso de entrada al sistema, para hacer uso del mecanismo de reconocimiento de huellas o iris ocular.

V Presenta la ventaja de que es el único aparato que identifica realmente al individuo y asegura que la persona que entra en las instalaciones está autorizada para ello.

X Por el contrario, su instalación es más costosa que las anteriores.

d. PERMISOS Y DERECHOS DE LOS USUARIOS

Cuando hablamos de **permisos**, hacemos referencia a la licencia para realizar algo, es decir, están vinculados a la autorización que tiene un usuario o grupo de usuarios sobre algún objeto o recurso.

Por otra parte, con **derechos** nos referimos a los beneficios o privilegios que se asignan a cuentas o grupos de usuarios para poder realizar una determinada acción.

Dentro de nuestro sistema, podemos otorgar **derechos** y **permisos** a los usuarios para que estos puedan realizar un conjunto de acciones **sobre** unos recursos.

Normalmente, el sistema otorga **derechos** para realizar acciones que prevalecen sobre los **permisos.**

Por ejemplo, el usuario *Local* puede tener **permisos** sobre un recurso en concreto, pero no sobre el ***Acceso** desde un equipo externo*, por lo que es posible restringir los **permisos** sobre ese **recurso** en una determinada situación.

Los **permisos** pueden heredarse a través de, por ejemplo, las carpetas, y restringirse con **permisos** más específicos sobre determinados recursos dentro de esa carpeta.

Entre los **permisos** más comunes que se dan a los recursos encontramos:

lectura o acceso,

escritura o modificación

y control total.

Cuando se asignan **permisos**, es común encontrarse con otros que afectan al propietario de un recurso o a un grupo en concreto (como un grupo de trabajo).

Los entornos Linux son un ejemplo de ello, ya que usan los siguientes tipos de permisos sobre los recursos:

- para el **propietario** del recurso,
- para el **grupo**
- y para el **resto de los usuarios**.

De esta forma es más fácil, por ejemplo, dar más **permisos** al creador de un recurso en concreto y no al resto de los usuarios.

GESTIÓN DEL INVENTARIO DE LOS REGISTROS DE USUARIOS, INCIDENCIAS Y ALARMAS

Cuando en la instalación tenemos un flujo de usuarios en el control de entradas y salidas, debemos disponer de una herramienta para llevar su control y gestión, así como de las incidencias producidas y las alarmas ocasionadas.

El mecanismo instalado para el **control del acceso** (depende de su complejidad) puede llevar, de forma adicional, una aplicación que controle dichas necesidades. En la actulidad, disponemos de numerosas aplicaciones para el mismo objetivo.

Durante todo este apartado hemos visto distintos tipos de alternativas para controlar la seguridad en el sistema, tanto medidas que se han centrado en el acceso propio del sistema como en el acceso a ciertos recursos.

Para la gestión de credenciales del usuario, podemos diferenciar dos conceptos (2):

AUTENTIFICACIÓN y **AUTORIZACIÓN**.

Métodos para la autentificación

La **autentificación** nos permite **identificar** a un usuario, ya sea a través de

- un usuario y contraseña
- un certificado
- u otros métodos.

El procedimiento más común es el primero que se ha mencionado.

En el método de la **contraseña de un solo uso**, cada vez que se desee acceder se utiliza una contraseña diferente

Por ejemplo, en las empresas bancarias, cada vez que se hace una operación sensible, mandan al usuario un mensaje con una serie de números y letras que van variando.

Otra alternativa a este método de acceso es el dispositivo ***secure token*** (token de seguridad), el cual es similar a la tarjeta personal,

pero está en otro dispositivo de almacenamiento donde solo se guarda la **contraseña.**

Puede ser una tarjeta, un *pendrive* o un llavero.

Autorización de usuarios

La **autorización** es la **herramienta** a través de la cual un **usuario** ya autentificado accede a ciertos recursos.

En los sistemas informáticos, es habitual pedir la autorización para operaciones que pueden causar algún daño en el sistema si se lleva a cabo por algún usuario no especializado.

Cuando se intenta centralizar toda la autentificación y autorización en un único sistema, se le denomina **Single Sign-On (SSO).**

La problemática de este tipo de mecanismos es que en cada red puede haber diferentes tipos de usuarios dentro de un grupo y diferentes aplicaciones que no se comportan igual entre varios usuarios.

Por ese motivo, en cada caso se necesitan unos determinados niveles de acceso a la aplicación.

Lo más normal es que cada aplicación tenga un método diferente para la gestión de usuarios. Por ejemplo, puede almacenarlos en una base de datos, lo que obliga a los usuarios a identificarse cada vez que se cambie de aplicación;

por eso aparece este tipo de mecanismo de acreditación, donde la base de datos de los usuarios es común a todo el sistema.

En este tipo de mecanismo se utiliza un **protocolo** de autentificación, entre los que destaca el **Kerberos**.

BUSCA EN LA WEB

El **Web Single Sign-On** es actualmente el sistema de gestión de autentificación de usuario más utilizado en el mercado.

Su relevancia se debe a que cada vez más hay aplicaciones web cuyas credenciales se quedan almacenada en internet y, por tanto, esta variante del método anterior posee la ventaja de no ocupar memoria en el sistema para almacenar los usuarios, especialmente cuando hay aplicaciones con un gran número de ellos.

Tema 1. Seguridad física y lógica

Cuando el sistema está implantado en una organización muy grande, con departamentos en varias sedes, es normal que trabajen con pocas aplicaciones comunes y muchas aplica- ciones individuales. Lo que se pretende en este caso es que el usuario pueda acceder a todas las aplicaciones con la misma credencial, lo que se denomina **identidad federada**. Además, dispone de su versión web, como la anterior, y recibe el nombre de **OpenId** para realizar la gestión de las credenciales de los usuarios desde internet.

¿SABÍAS QUE...?

El nombre del programa Kerberos hace referencia a Cerbero, can mitológico de tres cabezas que custodiaba la entrada al más allá.