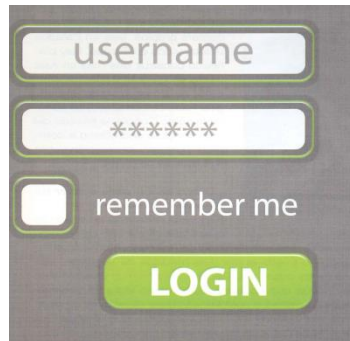


Seguridad lógica

Ut 3 1617



A login form with a dark gray background. It contains two input fields: the first is labeled 'username' and the second is labeled 'password' with a masked password '*****'. Below the password field is a checkbox labeled 'remember me'. At the bottom is a green button with the text 'LOGIN' in white capital letters.

username

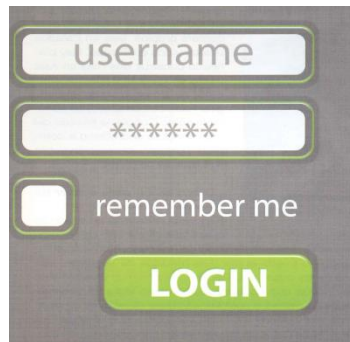
password *****

☐ remember me

LOGIN

Seguridad lógica

- Concepto de seguridad lógica
- Acceso a sistemas operativos y aplicaciones:
Contraseña y listas de control de acceso
- Acceso a aplicaciones por internet
- Autenticación y autorización de usuarios



A login form with a dark gray background. It contains a text input field labeled 'username', a password input field with six asterisks '*****', a checkbox labeled 'remember me', and a green button with the text 'LOGIN' in white capital letters.



Concepto de seguridad lógica

- En el tema anterior estudiamos la seguridad física.
- Aunque la protección física de los equipos informáticos es muy importante para cualquier empresa, no es menos importante la información que está almacenada en los mismos.



Concepto de seguridad lógica

- Antiguamente, cuando las organizaciones tenían sus datos y aplicaciones en grandes servidores de proceso por lotes de trabajo, garantizar la seguridad lógica suponía asegurar que sólo tenía acceso físico al sistema las personas autorizadas, (esto es, garantizar la seguridad física) y mantener una política robusta de copias de seguridad de los datos para poder recuperarlos en caso de incidente grave.



Concepto de seguridad lógica

Actualmente, sin embargo, con la enorme interconexión existente entre los sistemas con implantación masiva de Internet y las redes de datos:

- El tema de la seguridad lógica se ha convertido en el foco de atención de los departamentos de tecnología de las organizaciones.
- Los sistemas pueden ser comprometidos de forma remota por un atacante a través de una red mal protegida o aprovechando un sistema sin los adecuados sistemas de seguridad.



Concepto de seguridad lógica

Además, cada vez mas, se puede acceder a Internet desde multitud de dispositivos móviles (teléfonos, portátiles, tablets, etc.) y realizar desde allí actividades como adquirir bienes o servicios, reservar viajes, etc. Varios son los mecanismos de protección a los que estamos acostumbrados en la vida diaria:

- el patrón del teléfono móvil, la clave de acceso en los cajeros automáticos,
- El usuario y la contraseña para realizar compras online, etc.

Estas son algunas de las medidas de protección lógica.



Concepto de seguridad lógica

La **seguridad lógica** es el conjunto de medidas destinadas a la **protección de los datos y aplicaciones informáticas**, así como a **garantizar el acceso** a la información únicamente por **las personas autorizadas**.

Políticas de seguridad corporativa



La primera medida de seguridad lógica que debe adoptar una empresa es

establecer unas **normas claras** en las que se indique qué se puede y qué no

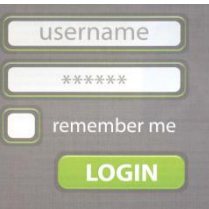
se puede hacer al operar con un sistema informático.

Estas normas marcan

las pautas generales de utilización del sistema y

configuran el marco de actuación de todos los usuarios.

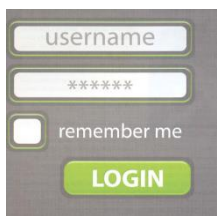
Políticas de seguridad corporativa



En sentido genérico, el conjunto de normas que definen las medidas de seguridad y los protocolos de actuación a seguir en la operativa del sistema

reciben el nombre de **políticas de seguridad corporativa** en materia informática.

Políticas de seguridad corporativa



Estas normas son **aplicables a toda la empresa**, por lo que todos los departamentos de la misma, deben estar implicados en su elaboración, ya que **todos van a tener que cumplirlas**.

Además, la política genérica engloba, a su vez, las distintas **normas específicas** aplicables a cada sector de la empresa, que estarán adaptadas, en cada caso, a los **niveles específicos de seguridad de cada sector**.

Políticas de seguridad corporativa

Entre las políticas de seguridad relacionadas con la seguridad informática tenemos las siguientes:

- **Instalación, mantenimiento y actualización de los equipos.**
- **Control de acceso a áreas críticas de la empresa y a recursos críticos del sistema.**
- **Utilización de recursos de las redes informáticas.**
- **Mantenimiento de las redes.**
- **Adquisición, instalación y actualización de software.**
- **Privacidad de la información.**
- **Autenticación de usuarios.**
- **Información de errores o de accesos al sistema.**
- **Contraseñas.**

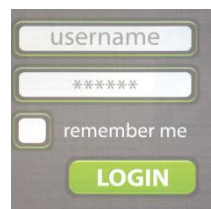


A login form with a grey background. It contains a text input field labeled 'username', a password input field with masked characters '*****', a checkbox labeled 'remember me', and a green 'LOGIN' button.

Políticas de seguridad corporativa

Algunas de las medidas o mecanismos establecidos en las políticas de seguridad son las siguientes:

- **Autenticación de usuarios:** sistema que trata de evitar accesos indebidos a la información a través de un proceso de identificación de usuarios que en muchos casos se realiza mediante un nombre de usuario y una contraseña.
- **Listas de control de acceso:** mecanismos que controlan que usuarios, roles o grupos de usuarios pueden realizar que cosas sobre los recursos del sistema operativo
- **Criptografía:** técnica que consiste en transformar un mensaje comprensible en otro cifrado según algún algoritmo complejo para evitar que personas no autorizadas accedan o modifiquen la información.
- **Certificados digitales** documentos digitales identificados por un número de serie único y con un periodo de validez incluido en el propio certificado mediante los cuales una autoridad de certificación acredita la identidad de su propietario vinculándolo con una clave pública.
- **Firmas Digitales:** Es el conjunto de datos, en forma electrónica consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante. Ejemplo :DNI electrónico.
- **Cifrado de unidades de disco o sistemas de archivos:** Medidas que protegen la confidencialidad de la información.

A graphic of a login form with a grey background. It contains a text input field labeled 'username', a password input field with masked characters '*****', a checkbox labeled 'remember me', and a green 'LOGIN' button.

Actividad 1 ut 3

- Contesta a las 5 preguntas
- Sube tus respuestas a la intranet.

2 >> Acceso a sistemas operativos y aplicaciones

Como hemos visto, para acceder a la información almacenada en un sistema informático:

1. En primer lugar hay que superar las **barreras físicas** de acceso.
 2. Una vez superadas estas barreras, el siguiente paso en materia de Seguridad será establecer unas **barreras lógicas** que impidan el acceso a nuestros datos:
- La **primera barrera lógica** que se puede establecer es la creación de mecanismos de control de acceso a la información.
 - Para ello, en vez de que al encender los equipos se pueda acceder directamente a todos los datos almacenados en los mismos, **una primera medida sería la creación de usuarios** para organizar la información, de forma que cada usuario únicamente pudiera acceder a la información de la cuenta para la que dispone de autorización.
 - **Las cuentas de usuario** permiten asignar a cada uno de ellos unos derechos y privilegios que restringirán las operaciones que este va a poder realizar dentro de un sistema informático, así como la posibilidad de rastrear dichas operaciones.
 - Como sistema de verificación de la identidad de cada uno de los usuarios se suele establecer la combinación entre un **nombre** identificativo (usuario, user, etc.), con la de una **contraseña** o password.
- Además, los equipos tienen instaladas distintas aplicaciones, respecto de las que se puede establecer un **control de usuarios integrado con el del sistema operativo o independiente del mismo**.
 - Si se trabaja en un entorno de red, es posible que, para acceder a algún recurso de la misma, se exijan unas **credenciales determinadas**, establecidas a través de las listas de control de acceso (**ACL, Access Control List**) que veremos en un epígrafe posterior.
 - Además, en las redes, los dispositivos de red, como **los routers, pueden servir de barrera lógica** impidiendo el acceso a determinadas zonas de la red para algunos usuarios (asignándoles un rango restrictivo de direcciones IP).

2.1 > Contraseñas

- Al igual que una llave permite abrir una cerradura que impide el paso a un lugar, las contraseñas son la llave que permite el acceso a aplicaciones y sistemas informáticos.
- En el ámbito informático podemos, por tanto, decir que una contraseña es un sistema de autenticación de usuarios compuesto por una combinación de símbolos (números, letras y otros signos).
- En determinados supuestos, basta con conocer la contraseña para controlar un dispositivo informático, como por ejemplo un teléfono móvil.
- Sin embargo, lo habitual es que un mismo sistema pueda ser usado por diferentes usuarios, por lo que cada contraseña va asociada a un usuario del sistema.
- De esta forma, para acceder al mismo, el usuario debe proporcionar su código identificador y la contraseña asociada a este y el sistema comprueba si ambos datos son correctos y si se corresponden entre sí, en cuyo caso habilita el acceso.

2.1 > Contraseñas

- De lo expuesto se deduce que **cuanto más robusta sea una contraseña mas difícil resultara acceder a la información protegida por la misma.**
- Una contraseña muy difícil de averiguar por alguien que no la conozca aporta seguridad a un sistema, **pero no basta.**
- En efecto, de nada sirve tener una contraseña muy difícil de averiguar si:
 - ~~la guardamos de forma que sea fácilmente accesible~~, si
 - ~~la revelamos~~ indiscriminadamente a terceras personas o si
 - ~~la comunicamos~~ sin tomar medidas de seguridad que impidan que otras personas puedan interceptar nuestra comunicación y obtenerla.
- Por tanto, como administradores de un sistema informático, **hay que ser estrictos a la hora de controlar las contraseñas de acceso al sistema desde todos los puntos de vista:** **fortaleza,** **almacenamiento** y **comunicación de las mismas.**

Amenazas para las contraseñas

- Si alguien intenta acceder a un sistema informático protegido con contraseña, previamente deberá averiguar esta,
- **Cuanto mas robusta sea una contraseña, mas difícil será averiguarla.**
- **Una combinación de cifras, números y otros caracteres hace que sea mas fuerte,** pero hay que tener en cuenta que los usuarios son seres humanos y tienden a establecer contraseñas fáciles de recordar, por lo que es habitual que los sistemas establezcan **restricciones que obliquen a los usuarios a cumplir unas determinadas normas a la hora de seleccionar sus contraseñas.**
- Ahora bien, por muy sencilla que sea la contraseña, los intrusos deben poner en práctica algún sistema para averiguarla.
- Existen diversos sistemas para tratar de averiguar las contraseñas, los mas habituales son los siguientes:
 - **Utilización de sniffers:** programas que registran la actividad de un equipo informático y pueden interceptar las comunicaciones “escuchando” para obtener datos como las contraseñas.
 - **Uso de Keyloggers** son programas o dispositivos cuyo fin es capturar las pulsaciones en un teclado, con lo que se pueden obtener las contraseñas que han sido escritas con ese teclado.
 - **Ataques por fuerza bruta:** consisten en probar todas las combinaciones posibles de caracteres hasta encontrar la clave que permite acceder al sistema. Por esto, cuanto mas larga sea la cadena de caracteres que tenga la clave mas se dificulta el acceso, pues mas tiempo requiere averiguar la contraseña: por ejemplo, e345Tj6k3L9934pR es mas fácil de averiguar que x4jT.
 - **Ataques por diccionarios** consisten en generar diccionarios con términos relacionados con el usuario y probar todas esas palabras como contraseñas para acceder a ese sistema. Suelen ser mas eficaces que los ataques por fuerza bruta, ya que los usuarios tienden a establecer como contraseñas palabras de su idioma, pues son más fáciles de recordar. Por eso, a igualdad de longitud de la cadena de caracteres de la contraseña, cuanto menos significado y más caracteres tenga esta, mas difícil será de hallar por ejemplo, hola es mucho mas fácil de averiguar que x4jT.
 - **Ataques por ingeniería social:** consisten en engañar a los usuarios para que proporcionen sus contraseñas a los intrusos, haciéndose estos pasar por amigos, empleados de un banco, técnicos. etc.

Políticas de seguridad en materia de contraseñas

Con el fin de evitar que las amenazas expuestas en el apartado anterior sean efectivas y que un usuario malintencionado pueda acceder a los datos de un sistema informático, es esencial que los usuarios y empresas establezcan unas políticas de seguridad relativas a las contraseñas,

- Establecimiento de las contraseñas
 - Las contraseñas deben elegirse en función de su idoneidad para proteger la información, no en función de su facilidad para ser recordadas por el usuario.
 - Como se adelantó en la página anterior, una adecuada política de seguridad prestara atención en fijar unas normas para la elección de contraseñas que dificulten los ataques por diccionario o por fuerza bruta.

Para ello, las normas básicas son las siguientes:

- ~~NO deben ser o contener palabras usuales ni relacionadas con el entorno del usuario~~, como por ejemplo: nombres de mascotas, fechas de cumpleaños, número del DNI, etc.
- ~~No deben ser palabras con significado~~, por ejemplo, “alimento”.
- La contraseña debería ser una combinación de mayúsculas, minúsculas, números y otros caracteres, por ejemplo: aX4t\$5#.
A mayor variedad de símbolos utilizada. mayor dificultad para averiguar la contraseña.
- La longitud de la contraseña debería ser de **ocho caracteres como mínimo**.
- Hay que evitar que el usuario **utilice la misma contraseña en varios sitios**, por ejemplo, que se utilice la misma contraseña para entrar a las aplicaciones de la empresa, al correo y a redes sociales.
- Se deben **cambiar las contraseñas** proporcionadas por defecto al registrarse por Internet en cualquier servicio.

Establecimiento de contraseña segura

- El establecimiento de una contraseña que cumpla con los requisitos de seguridad puede **generar cierta ansiedad** por parte los usuarios que van a trabajar en el sistema.
- Una posible solución para crear contraseñas que cumplan con todos los requisitos y sean fáciles de recordar para el usuario es elaborarlas **a partir de la primera letra o sílaba de cada palabra que integre una frase.**
- Por ejemplo, partiendo de la frase:
“**L**a **s**elección **e**spañola **g**anó **e**l **m**undial **d**e **S**udáfrica **e**n **2011!**”,
se pueden tomar las primeras letras de cada palabra, los números y el signo de admiración para crear una contraseña segura como la siguiente:
LsegemdSe2011!

Comunicación de las contraseñas

- Para evitar los ataques de ingeniería social, se debe vigilar la comunicación de las contraseñas por parte del usuario, instruyéndole en la desconfianza del restablecimiento de contraseñas o de números de tarjeta bancaria, etc., mediante correos electrónicos o encuestas telefónicas.
- Además se deben tomar medidas para que los medios a través de los que se transmita la información (cable, WiFi, etc.) sean seguros, encriptando la información para dificultar el acceso a la misma en caso de que sea interceptada.

Gestores de contraseñas

- Existen programas de gestión de contraseñas que permiten almacenar todas nuestras contraseñas de forma cifrada y segura.
- En estos programas se establece una contraseña maestra para acceder a ellos de forma que, en lugar de tener que recordar innumerables contraseñas, basta con recordar la que da acceso al programa.
- Por ejemplo KeePass Password Safe (<http://keepassinfo/>)
- es una aplicación de código abierto y disponible en varias plataformas.

Combinaciones de contraseñas

- Teóricamente, un ataque de fuerza bruta *tendrá éxito siempre y cuando se le deje actuar el tiempo suficiente.*
- Por ello, cuantas mas combinaciones de contraseñas tenga que probar y menos tiempo se le dé para ello, mas difícil será que averigüe la contraseña correcta.
- Por ejemplo, una contraseña de seis caracteres compuesta por las letras en minúscula del alfabeto castellano tendría $27^6 = 357.420.489$ combinaciones.
- Si *subimos el número de caracteres a ocho y utilizamos mayúsculas y minúsculas y los signos de puntuación mas usuales, el número de combinaciones es de más de mil quinientos billones.*
- Si además, *cambiamos la contraseña cada tres meses*, el atacante solo dispondrá de ese tiempo para probar todas las posibles combinaciones.

Almacenamiento de las contraseñas

- De nada sirve la fortaleza de una contraseña si esta no se almacena correctamente.
- Por ello, no se deben anotar las contraseñas ni en papel ni en archivos de texto plano en el ordenador.
- Si se quieren almacenar contraseñas en el ordenador, se debe recurrir al uso de programas gestores de contraseñas.
- No obstante, cuando se lleva una política de contraseñas robusta, con cierta frecuencia ocurre que se pierde la contraseña del usuario administrador del sistema, ya sea porque se olvida o porque se almacené mal en el gestor de contraseñas.
- En el caso de sistemas Linux, es posible regenerarla si se tiene acceso al sistema desde una consola.
 - Para ello, basta con reiniciar el sistema y seleccionar el modo de arranque en modo monousuario.
 - Este modo, que solo levanta unos servicios mínimos del sistema y, por ejemplo, no habilita la red, si proporciona acceso por consola como usuario root sin necesidad de introducir contraseña.
 - Una vez arrancado, se modifica la contraseña de root desde el modo monousuario y se reinicia normalmente.
- Por todo esto, Seguridad física y lógica deben ir de la mano.
- Como vemos, establecer una política segura de contraseñas puede no servir de nada si un atacante logra tener acceso físico a la consola del servidor y reiniciarlo.

Papel del administrador del sistema

En todo caso, como administradores de sistemas, si bien hay que prestar especial atención en la formación al usuario para que cumpla todas las normas propuestas, habrá que tomar medidas adicionales para el caso de que estos no cumplan dichas normas, “forzándoles” a tomar ciertas medidas

de seguridad:

- Estableciendo un número máximo de intentos para acceder al sistema.

Por ejemplo, si el usuario introduce tres veces seguidas una contraseña incorrecta, se bloquea el acceso y solo puede ser desbloqueado por el administrador.

- Obligando al usuario a que establezca contraseñas con un mínimo de ocho caracteres alfanuméricos que combinen, al menos, una mayúscula, una minúscula, un número y un signo de puntuación.
- Obligando al usuario a cambiar la contraseña cada cierto tiempo (por ejemplo, cada tres meses).
- Impidiendo al usuario repetir las tres últimas contraseñas utilizadas.

- Una herramienta que permite al administrador gestionar las contraseñas de un sistema son las cuentas de usuario.
 - Estas cuentas permiten conceder unos determinados permisos y privilegios a cada usuario, el cual solo podrá utilizar los recursos del sistema en función del rol que el administrador le haya asignado.
- Las políticas relacionadas con las contraseñas se gestionan, en los sistemas Windows, desde la consola de Directivas de seguridad local, que es una herramienta muy valiosa desde el punto de vista de la seguridad, ya que afina al máximo los privilegios de los usuarios y diversas directivas relacionadas con la seguridad.

Papel del administrador del sistema

Eso si, el administrador del sistema deberá tener en cuenta **que el establecimiento de estas medidas puede provocar que, ante la dificultad de recordar las nuevas contraseñas** que el sistema le obliga a crear y cambiar constantemente, el usuario caiga en la tentación de apuntarlas en papel o en un archive en texto plano.

Aquí sería especialmente **recomendable el uso de un programa gestor de contraseñas.**

En cualquier caso, habrá que evaluar la criticidad de los sistemas a proteger y **llegar a un compromiso entre la facilidad de gestión y el nivel de seguridad requerido.**

Una política muy robusta de contraseñas lleva aparejados frecuentes incidentes de tipo olvido de contraseñas, bloqueo de usuarios por sucesivos intentos fallidos, etc. que pueden hacer que no merezca la pena utilizarla en sistemas no críticos.

Actividad 2 ut 3

Administración de políticas de contraseñas

El administrador de sistemas de una empresa ha decidido aplicar una política de contraseñas que controle la elección, utilización y administración de las mismas, para evitar posibles intrusiones en el sistema. La política determina que:

- Cada usuario tendrá una contraseña establecida por defecto, que deberá cambiar por una de su elección en el próximo inicio de sesión.
- Las contraseñas que se elijan por los usuarios deberán ser de diez caracteres como mínimo y tendrán una vigencia máxima de un mes.

- Haz un tutorial de cómo realizar dichas tareas si todos los usuarios utilizan Windows 7, versión Professional.