



Ut 3

Parte II

En ocasiones, para restringir el acceso a los recursos del sistema no es suficiente con la utilización de perfiles de usuario y la creación de grupos, sino que es necesario realizar **un ajuste más riguroso**.

Por ejemplo, puede existir un directorio donde físicamente deban acceder **dos usuarios que pertenecen a grupos distintos** para realizar cosas diferentes, etc.

Para estos puestos se utilizan las listas de control de acceso o **ACL (Access Control List)**, cuya utilización variará en función del sistema operativo instalado, aunque los fundamentos son los mismos.

- **Las listas de control de acceso son una herramienta que permite controlar qué usuarios pueden acceder a las distintas aplicaciones, sistemas, recursos, dispositivos.**

Listas de control de acceso

- Las ACL son un mecanismo básico para proporcionar seguridad a las redes de datos **pudiéndose utilizar tanto para restringir y controlar el acceso desde el punto de vista de la red (proporcionando seguridad a las redes de datos)**, como desde el punto de vista del sistema operativo para realizar esas mismas tareas sobre distintos recursos del sistema,
- Por un lado, los elementos constitutivos de la red suelen **utilizar ACL basadas en direcciones de red, direcciones IP o direcciones MAC** para configurar las políticas de acceso o bloqueo a los recursos,
- Así, mediante el establecimiento de políticas de seguridad en los firewall que protegen la red, puede permitirse el acceso desde o hacia solo determinados sistemas, pueden **bloquearse todos los puertos que no vayan a ser explícitamente necesarios, etc.**

Las **ACL** también se aplican masivamente en servicios básicos de red tales como:

- **Proxy** (para controlar quién puede salir a Internet o quién puede visitar qué páginas),
- Servidores **DNS** (para evitar ataques desde direcciones IP no identificadas),
- **Servidores de correo electrónico** (para evitar ataques por spam desde direcciones IP no autorizadas),
- etc...

ACL

- En los routers se pueden establecer listas de control de acceso de las siguientes formas:

- **Por protocolo:**
 - Se define una ACL para cada protocolo.
- **Por interfaz:**
 - Se define una ACL para cada interfaz del router.
- **Por dirección IP:**
 - Se define una ACL para restringir el tráfico IP.

ACL en los router

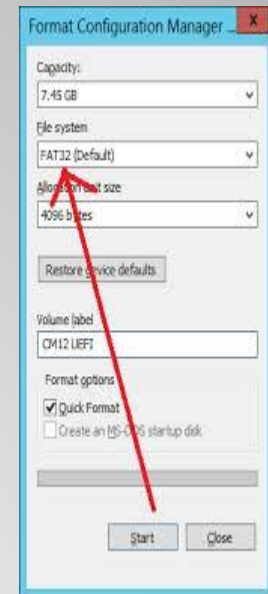
- — Posibilidad de **mejorar el rendimiento de la red limitando determinado tráfico.**
 - Por ejemplo, se puede impedir que los empleados de una oficina descarguen o visualicen ficheros de video. Los ficheros de video ocupan mucho ancho de banda y pueden llegar a colapsar la red.
- — Posibilidad **de permitir o denegar el acceso de equipos a ciertas Zonas de la red.**
 - Por ejemplo, los empleados que trabajan en una zona de red (caracterizada por un rango de direcciones IP) no deberían acceder a la zona de red donde trabaja el personal de administración.
- — Permiten que **no se ejecuten determinados comandos por la red destinados a fines malintencionados**
 - Instalación de troyanos, comandos del sistema, etc.).

- A cambio, presentan el inconveniente de.
 - La exhaustividad en el nivel de control complica bastante la administración de la seguridad del sistema.

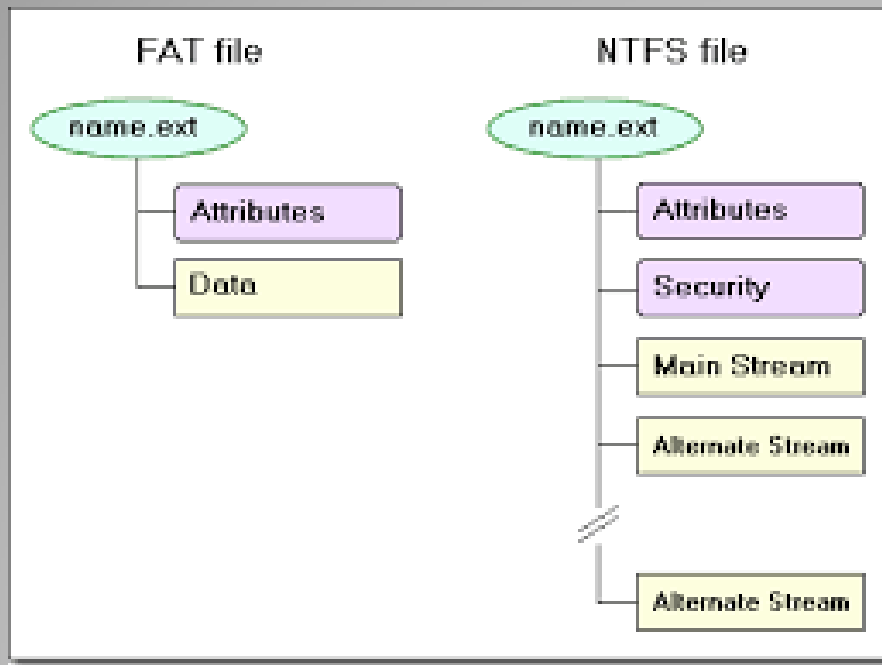
Por tanto, habría que valorar hasta qué punto las ventajas superan a los inconvenientes en cada supuesto.

Ventajas e inconvenientes de las ACL :

- En sistemas Windows, las opciones de compartición de recursos van a depender del sistema de archivos con el que se trabaje.
- **FAT32 únicamente** permite la **compartición de recursos a todos** los usuarios o **prácticamente a ninguno.**



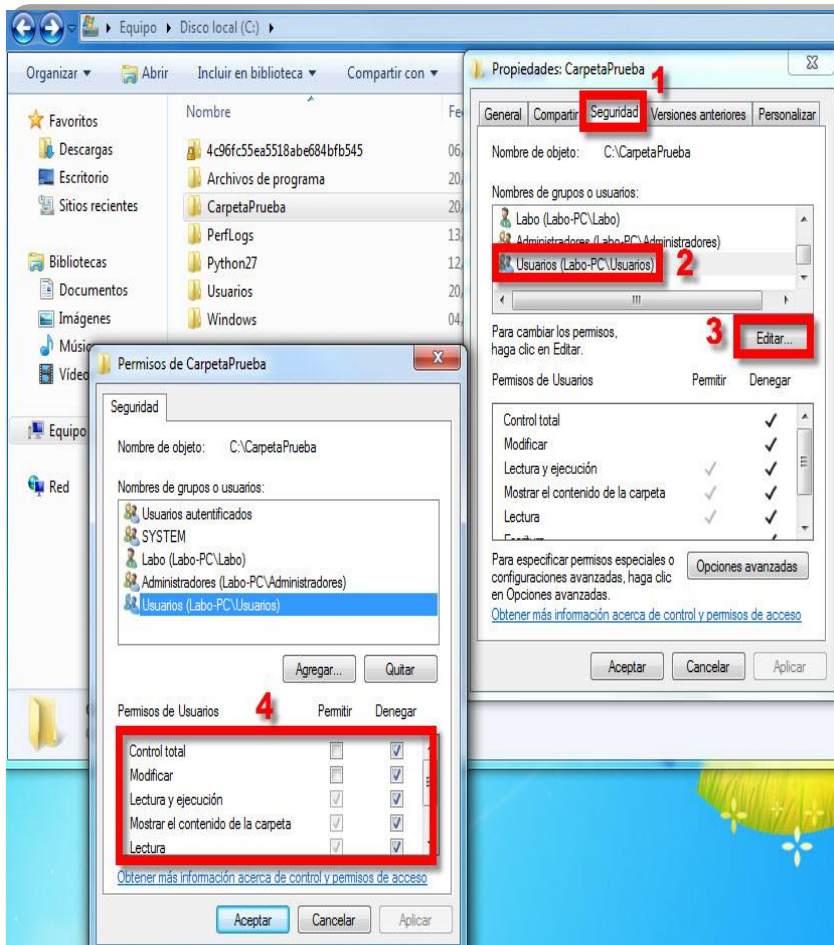
ACL on Windows



- Para cada usuario que tiene acceso a un directorio o a un fichero existe una entrada de acceso que indica el tipo de operaciones que puede realizar.

- NTFS permite aprovechar al máximo las ventajas de la compartición de recursos y la asignación de permisos avanzada.
 - En los discos o volúmenes formateados con NTFS, **cada fichero y cada directorio tiene una lista de control de acceso o permisos NTFS.**

ACL en Windows

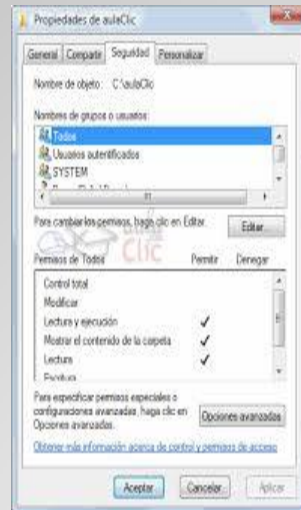


Windows distingue dos tipos de privilegios de acceso:

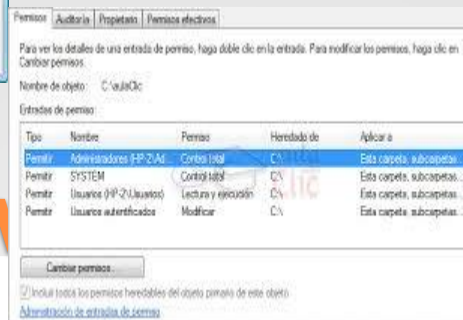
- **Los permisos:** establecen la **forma de acceder** a un objeto concreto, por ejemplo,
 - escribir un archivo NTFS.
- **Los derechos:** establecen qué **acciones se pueden realizar** en el sistema, como por ejemplo.
 - iniciar sesión.

ACL en Windows

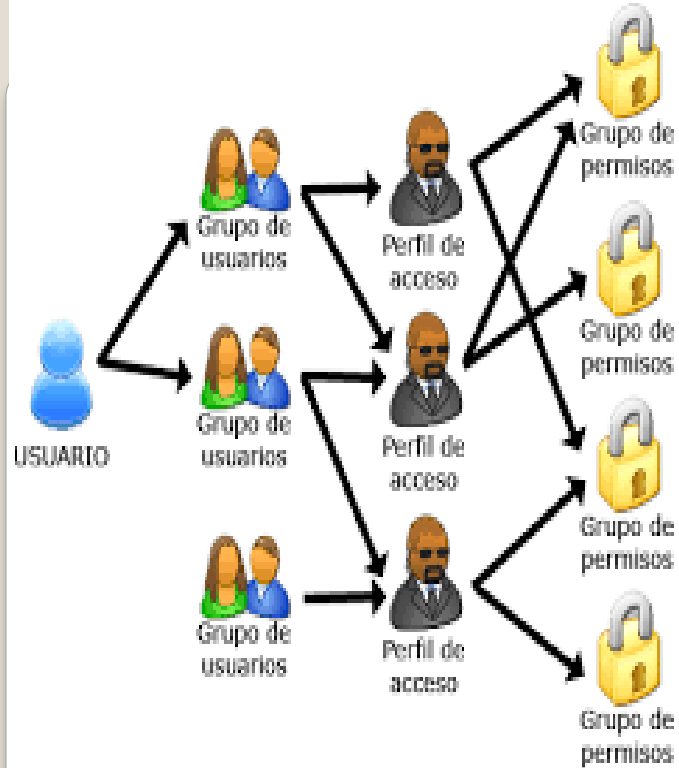
- El **propietario** de un recurso (o un administrador) **asigna permisos** sobre dicho recurso a través del cuadro de diálogo de propiedades del mismo.



- Por ejemplo, si en la carpeta D:/Programas se hace clic sobre ella con **el botón secundario** del ratón, se abre el cuadro de diálogo **Propiedades**.
- Si se selecciona la pestaña "**Seguridad**" se ven los usuarios que tienen permisos sobre ella.



ACL Window

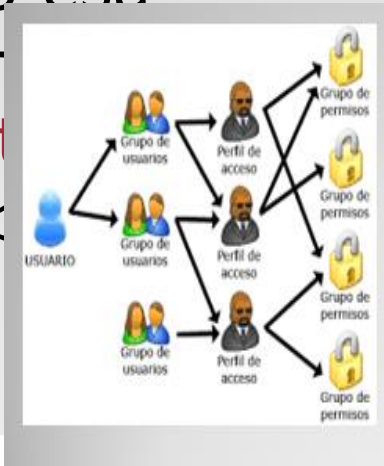


- Desde allí también se puede configurar la asignación de los usuarios a grupos del sistema.

ACL Windows

- Los administradores configuran los **derechos y privilegios** del usuario dentro del sistema a través de la consola **Directiva de seguridad local**, a la que se accede desde **Panel de control / Herramientas administrativas**.

- Los permisos sobre **ficheros son distintos** de los **que** se pueden aplicar a los **directorios**.
- Unos y otros tienen un **usuario propietario**, que es quien ha creado esa carpeta o fichero, **quién tiene control total** sobre el objeto.



- Para **cada objeto** (fichero, directorio, recurso) se establece **una lista de usuarios y/o grupos** y a **cada uno** de ellos se les aplican los **permisos pertinentes**.

Esta lista se denomina **ACL (Access Control List)**.

- Cada una de las entradas que forman estas listas recibe el nombre de **ACE (Access Control Entry)**.

ACL Windows

En un sistema en red debidamente configurado, el administrador del sistema se encarga de establecer los permisos, los derechos y los privilegios del usuario.

- Los usuarios normales, no administradores, deberían tener privilegios limitados o nulos dentro del sistema y no se les debería permitir la realización de acciones como:
 - la instalación de programas
 - modificaciones en el sistema.
- Los usuarios normales, tan solo deben ser propietarios de sus directorios de trabajo en zonas de trabajo seguras (directorios en la red, directorios locales, etc.),

ACL Windows

- En Linux, todos los usuarios pertenecen a un grupo principal

(que lleva el nombre de ese usuario o se le puede asignar 0110 existente) y, además, pueden pertenecer a

otros secundarios ■

ACL Linux

- El usuario administrador del sistema se denomina **root** y tiene todos los privilegios del sistema,
 - Creación de nuevos usuarios.
 - El cambio de las contraseñas de los otros usuarios o
 - La ejecución de comandos privilegiados del sistema.

Desde el punto de vista de la seguridad, **no es recomendable trabajar con este usuario**, sino con otro con menos privilegios.

- Cada fichero o directorio pertenece a un usuario y, por tanto, a uno de los grupos a los que pertenece el usuario.
- Los permisos de cada fichero o directorio se ajustan para el usuario propietario (u), para su grupo (g) y para el resto (o).
 - Estos permisos aplicados implican que el recurso puede leerse (r), ser editado (w) o ser ejecutado (x), además existe un cuarto campo que indica la máscara.
- Los permisos sobre ficheros y directorios **se establecen mediante el comando chmod**, usando la notación UGO o la notación octal.
- Por ejemplo:
 - `chmod g-wx, o-rwx nombre_fichero` es lo mismo que `chmod 740 nombre_fichero`, lo que significa que el propietario tiene todos los permisos, los usuarios del grupo solo permiso de lectura y el resto de usuarios ningún permiso.

- - La primera columna contiene un grupo de letras que indican lo siguiente:
 - la primera letra indica el tipo de fichero (d indica directorio),
 - las tres siguientes letras indican los permisos (r lectura, w escritura, x ejecución) del usuario (tecnico1) sobre el directorio (por ejemplo Descargas);
 - los tres siguientes caracteres indican los permisos (r-x, tiene permisos de lectura y ejecución pero no de escritura) del grupo at que pertenece el usuario (técnicos);

- - La tercera columna hace referencia al usuario propietario del fichero o directorio, en este caso tecnico1.
- - La cuarta columna hace referencia al grupo al que pertenece el usuario propietario (tecnicos).
- - La ultima columna contiene el nombre del directorio o fichero (Descargas, Documentos, etc.).

Establecimiento de permisos en

Linux

los tres siguientes indican los permisos del resto de usuarios (r-x, tiene permisos de lectura y ejecución pero no de escritura).

```
total 32
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago 6 19:43 Descargas
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago 6 19:43 Documentos
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago 6 19:43 Escritorio
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago 6 19:43 Imagenes
```


- En ocasiones, **estos permisos no serán suficientes para establecer restricciones a los usuarios** de un sistema, por ello se utilizan las ACL.
- Por ejemplo, puede existir **un directorio al que interese dar acceso a todos los usuarios de dos grupos concretos, manteniéndolo restringido para el resto de los usuarios.**
- En este caso, el permiso de grupo solo nos permitiría darle acceso al grupo propietario, dejando al otro fuera, mientras que el permiso others sería demasiado amplio, pues daría acceso a todos los grupos
- En Linux, si las ACL están habilitadas, para activarlas en una partición o directorio hay que **añadir la palabra acl** al final de la línea correspondiente a dicha partición en el fichero `/etc/fstab` . A continuación tendríamos que desmontar y montar la partición:

```
#mount -O remount -o acl /dev/sda3  
/home
```

ACL en Linux

- Una ACL esté compuesta por varias entradas, cada una de las cuales especifica los permisos de acceso a un recurso para un usuario o un grupo, utilizando una combinación de los permisos tradicionales de lectura (r), escritura (w) y ejecución (x). Estas entradas son:
- La categoría: usuario (u), grupo (g), otros (o) o máscara (m).
- UID(identificador de usuario) o GID (identificador de grupo) del usuario o grupo afectado.
 - Este campo puede estar vacío, en cuyo caso la ACL se vincula al usuario propietario o al grupo propietario.
- Cadena con los permisos asignados.
- El conjunto de la categoría y el identificador del usuario o grupo definen el tipo de entrada.

ACL en Linux

Tipo de entrada	Visualización	Descripción
<i>owner</i>	u[ser]::rwx	Privilegios de acceso del propietario.
<i>group</i>	g[roup]::rwx	Privilegios de acceso del grupo propietario.
<i>other</i>	o[ther]::rwx	Privilegios que no corresponden a ninguna entrada (otros).
<i>named user</i>	u[ser]:name:rwx	Privilegios de acceso para los usuarios identificados por una ACL.
<i>named group</i>	g[roup]:name:rwx	Privilegios de acceso del grupo identificado por una ACL.
<i>mask</i>	m[ask]::rwx	Privilegios máximos para los tipos <i>named user</i> , <i>named group</i> .

- Las tres primeras entradas de la tabla se conocen como **ACL estándar** y coinciden con la gestión simple de los permisos: owner, group y other.
- Las otras tres se conocen como **ACL extendida**, que proporciona mayor flexibilidad, dado que permite otorgar permisos a un usuario concreto indicando su nombre (*named user*), a un grupo concreto indicando su nombre (*named group*) o utilizando una máscara (*mask*).

ACL en
Linux

Tipo de entrada	Visualización	Descripción
<i>owner</i>	u[ser]::rwx	Privilegios de acceso del propietario.
<i>group</i>	g[roup]::rwx	Privilegios de acceso del grupo propietario.
<i>other</i>	o[ther]::rwx	Privilegios que no corresponden a ninguna entrada (otros).
<i>named user</i>	u[ser]:name:rwx	Privilegios de acceso para los usuarios identificados por una ACL.
<i>named group</i>	g[roup]:name:rwx	Privilegios de acceso del grupo identificado por una ACL.
<i>mask</i>	m[ask]::rwx	Privilegios máximos otorgados a <i>named user</i> , <i>group</i> y <i>named group</i> .

- El orden de aplicación de reglas es el siguiente: *owner*, *named user*, *owning group*, *named group* y *other*.
- La máscara se aplica sobre cualquier entrada, a excepción de *owner* y *other*, esto es, actúa sobre las entradas de tipo *named user*, *owning group* y *named group*.

ACL en Linux

- ¿Cómo se accede a la consola de Directiva de Seguridad Local en Windows?
- Indica 3 directivas de seguridad de contraseñas que establecerías en una empresa de 1150 empleados.
 - Hay 5 tipos de usuarios:
 - Operarios
 - Aprendices
 - Maestros de Taller
 - Ingenieros
 - Directivos
 - Cada tipo pertenece a un grupo.

Actividades propuestas

Utilización de ACL en Linux

En primer lugar instalamos el soporte de ACL, ejecutando como root alguno de los siguientes comandos en funcion de la distribucion Linux que tengamos instalada:

- *apt-get install acl* para distribuciones tales como Debian, Ubuntu, etc.
- *yum install acl* para distribuciones tales como en Red Hat, Fedora, etc.

Creamos dos usuarios: tarzan, que pertenece al grupo jungle, y jane, que pertenece al grupo city.

```
groupadd jungle
groupadd city
useradd -m -G jungle
tarzan
useradd -m -G city
jane
```

Práctica 4

Creamos dentro de nuestro directorio /home un directorio llamado mydir con permisos rwxrwx- — —.

```
chmod 0770 mydir
```

Creamos los ficheros docum1 y docum2, con permisos rwxrwx— — -

```
chmod 0770 docum*
```

Práctica 4

Asignar permisos de lectura, escritura y ejecución al grupo jungle para el directorio mydir

```
setfacl -R -m g:  
jungle:rwX  
/home/alumno/mydir
```

Al grupo city le asignamos permisos de lectura y ejecución para el directorio mydir— — -

```
setfacl -R -m  
g:city:rw  
/home/alumno/mydir
```

Práctica 4

Asignamos permisos de lectura, escritura y ejecución al usuario jane para el fichero docum1

```
setfacl -m u:jane:rw  
/home/alumno/mydir/docum1
```

(El usuario jane no puede leer ni escribir ni ejecutar el fichero docum2)

Al grupo city le asignamos permisos de lectura y ejecución para el directorio mydir— — -

```
setfacl -R -m  
g:city:rw  
/home/alumno/mydir
```

Práctica 4

**Añadimos un nuevo usuario
llamado john al grupo jungle**

**comprobamos que puede entrar al directorio
mydir y que puede leer o modificar los
ficheros.**

Práctica 4

Quitamos los permisos de lectura y ejecución al directorio mydir al usuario llamado john

comprobamos que john no puede acceder a dicho directorio mydir

```
setfacl -m u : john :w  
/home/alumno/mydir
```

Práctica 4

Crear una mascara ACL en el directorio mydir que indique que los permisos máximos que tendrá en el mismo cualquier usuario que no sea el propietario 0 el resto serán de lectura o ejecución

Comprobamos que los usuarios creados (tarzan, john o jane) no pueden crear archivos en el directorio mydir debido a la mascara, que elimina el permiso de escritura a cualquier usuario distinto del propietario u otros.

```
setfacl -m m: :rx  
/home/alumno/mydir
```

Práctica 4

Internet es una fuente inagotable de recursos y de aplicaciones que nos facilitan mucho la vida.

- Varios son los tipos de aplicaciones a las que el usuario puede acceder, algunas de ellas no requieren ninguna credencial para su consulta o para trabajar con ellas, pero otras si.
- Es importante garantizar y proteger la identidad de los usuarios cuando se identifican en una página web.
- Por otro lado, se deben configurar las páginas web de modo que la transferencia de datos con los usuarios sea segura, especialmente, si estos datos son sensibles.

Acceso a aplicaciones por Internet

7

Hay siete normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Acceso a aplicaciones por Internet

Norma

1

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

- **Mantener actualizados tanto el sistema operativo como el navegador** y, dependiendo del sistema operativo instalado, disponer de un antivirus actualizado. Los bugs detectados y no corregidos mediante las actualizaciones son auténticos agujeros de seguridad.

Acceso a aplicaciones por Internet

Norma

2

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Las ACL :

La importancia de una correcta administración de los nombres de usuario y las contraseñas.

(Todo lo dicho hasta ahora en esta unidad respecto a los sistemas operativos, aplicaciones y redes de comunicaciones.)

Acceso a aplicaciones por Internet

Norma

3

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

- Desconfiar de las webs en las que para regenerar una contraseña olvidada permiten introducir una cuenta de correo a la que enviar la nueva contraseña debido a que, si alguien averiguara el identificador del usuario, podría conseguir fácilmente su contraseña.

Acceso a aplicaciones por Internet

Norma

4

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Acceder a las distintas aplicaciones desde un ordenador seguro si los datos son muy sensibles (fundamentalmente transacciones económicas): se debe evitar acceder desde ordenadores públicos (locutorios, bibliotecas, etc.), así como desde conexiones WiFi abiertas.

Acceso a aplicaciones por Internet

Norma

5

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

- **No facilitar por correo electrónico ni telefónicamente las contraseñas, ni modificarlas por estas vías:** la Administración Pública y las empresas como los bancos nunca solicitaran realizar operaciones de este tipo. Los correos que dicen ser de un banco y contienen un enlace a una pagina donde se solicitan claves suelen ser una trampa para conseguir estas claves.

Acceso a aplicaciones por Internet

Norma

6

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

- **No acceder nunca a través de enlaces** a la pagina web de una empresa u organismo público para realizar un tramite. Si se quiere acceder a estas paginas hay que teclear siempre en el navegador la dirección, para evitar ser victima del phishing.

Acceso a aplicaciones por Internet

Norma

7

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

- **Cerrar la sesión correctamente**, usando el vinculo Salir, Cerrar Sesión o similar de la pagina web en la que nos hallarnos registrado, sea un banco o una cuenta de correo pues, en caso contrario, puede que la conexión quede abierta. Además, para mayor seguridad, después de cerrar cada sesión se deberían borrar los archivos temporales y el historial de navegación.

Acceso a aplicaciones por Internet

Hay unas normas generales aplicables a todas las aplicaciones web que ponen especial énfasis en el eslabón mas débil de la cadena a efectos de seguridad, el usuario:

7 Mantener actualizados tanto el sistema operativo como el navegador y, dependiendo del sistema operativo instalado, disponer de un antivirus actualizado. Los bugs detectados y no corregidos mediante las actualizaciones son auténticos agujeros de seguridad.

La importancia de una correcta administración de los nombres de usuario y las contraseñas. ACL.

Desconfiar de las webs en las que para regenerar una contraseña olvidada permiten introducir una cuenta de correo a la que enviar la nueva contraseña debido a que, si alguien averiguara el identificador del usuario, podría conseguir fácilmente su contraseña.

Acceder a las distintas aplicaciones desde un ordenador seguro si los datos son muy sensibles (fundamentalmente transacciones económicas): se debe evitar acceder desde ordenadores públicos (locutorios, bibliotecas, etc.), así como desde conexiones WiFi abiertas.

No facilitar por correo electrónico ni telefónicamente las contraseñas, ni modificarlas por estas vías: la Administración Pública y las empresas como los bancos nunca solicitaran realizar operaciones de este tipo. Los correos que dicen ser de un banco y contienen un enlace a una pagina donde se solicitan claves suelen ser una trampa para conseguir estas claves.

No acceder nunca a través de enlaces a la pagina web de una empresa u organismo público para realizar un tramite. Si se quiere acceder a estas paginas hay que teclear siempre en el navegador la dirección, para evitar ser victima del phishing.

Cerrar la sesión correctamente, usando el vinculo Salir, Cerrar Sesión o similar de la pagina web en la que nos hallarnos registrado, sea un banco o una cuenta de correo pues, en caso contrario, puede que la conexión quede abierta. Además, para mayor seguridad, después de cerrar cada sesión se deberían borrar los archivos temporales y el historial de navegación.

Acceso a aplicaciones por Internet

Phishing

- Fraude que consiste en suplantar la identidad de personas o entidades de Internet para conseguir claves de acceso a su nombre de usuario y contraseña de operación web.

De: **Equipo de Gmail** <communications_cs_eses@gmail.com>
Fecha: 22 de enero de 2012 00:18
Asunto: Cuenta Desactivada
Para: vx@gmail.com

Gmail: correo electrónico de Google - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

M Gmail: correo electrónico de G...

login.gmail.com.msg11.info/accounts2/ServiceLogin2.php?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2F




Google

¿Es la primera vez que utilizas Gmail? **CREAR UNA CUENTA**

Gmail

La visión del correo electrónico de Google.

Gmail está basado en la idea de hacer que el correo electrónico resulte más intuitivo, eficiente y útil, e incluso divertido. Después de todo, Gmail tiene:

-  **Mucho espacio**
Más de 2757.272164 megabytes (y sigue en aumento) de almacenamiento gratuito.
-  **Menos spam**
Evita que los mensajes no deseados lleguen a la bandeja de entrada.
-  **Acceso para móviles**
Para leer mensajes de Gmail desde tu teléfono móvil, introduce <http://gmail.com> en el navegador web de tu móvil. [Más información](#)

[Acerca de Gmail](#) [Nuevas funciones](#) [Crear una nueva dirección de Gmail](#)

Acceso Google

Nombre de usuario
[redacted]@gmail.com

Contraseña

Acceso

[¿No puedes acceder a tu cuenta?](#)
[Salir y acceder como otro usuario](#)

Te damos la bienvenida a la nueva página de acceso de Google. [Más información](#)

© 2011 Google [Gmail para organizaciones](#) [Política de privacidad](#) [Política del programa](#) [Términos de uso](#)

URL FALSA

VeriSign

- Es una empresa proveedora de servicios de autenticación que actúa como autoridad de certificación a nivel mundial.
- Emite certificados SSL para la protección de sitios en Internet.
- Por ello, si una conexión está verificada por esta empresa, ello indica que es un servicio de confianza.

Plataformas de pago

- Una plataforma o pasarela de pago es un servicio de comercio electrónico que autoriza los pagos realizados a través de Internet.
- Cifra los datos sensibles, como número de cuenta o de tarjeta.
- Una de las mas utilizadas es PayPal.

Asegurar el canal

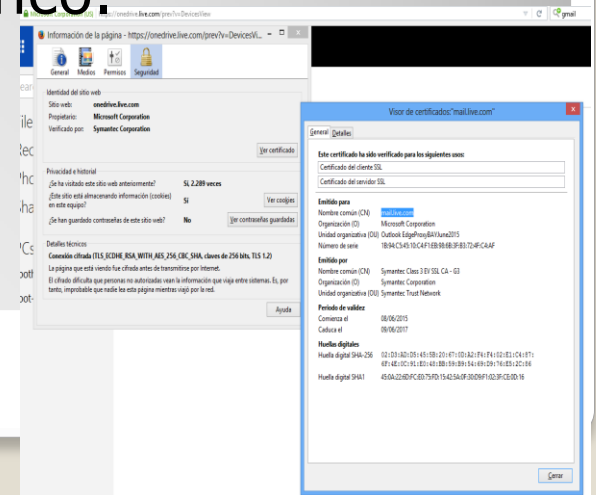
HTTPS

- Es importante asegurarnos de que el canal por el que se accede a la web en cuestión es fiable.
- Para ello, basta con observar en la barra de navegación que la dirección web comienza por https en vez de por http



- Eso indica que la conexión es segura.
- Además, en el navegador suele aparecer un candado cerrado indicando que la conexión es cifrada.
- Al hacer doble clic sobre él aparece el certificado de identidad del banco.

¿Es la web fiable?



El protocolo https (hyper text transfer protocol secure)

- Está basado en el http.
- Su finalidad es proporcionar un plus de seguridad a la transmisión de datos sensibles.
- Este protocolo crea un canal seguro a base de cifrar los datos que se están transmitiendo, de modo que si se interceptan las comunicaciones físicamente se puede acceder a un código que el intruso no puede interpretar.

Certificados digitales

- La esencia de las transacciones de datos comerciales y administrativas realizadas por vía electrónica es la realización de un acto con eficacia jurídica :
 - una declaración tributaria,
 - una reserva de hotel,
 - una transferencia bancaria, etc.
- Tan importante como la seguridad en la transmisión de los datos es la acreditación de la identidad de las partes intervinientes.
- Los certificados digitales, (que veremos en otras unidades posteriores) realizan dicha acreditación.

El protocolo https

AUTORIDADES DE CERTIFICACIÓN

- En la emisión y gestión de estos certificados son esenciales las autoridades de certificación.
- Instituciones a las que uno o mas usuarios confían la creación y asignación de certificados y/o las claves de usuario.
- Por ejemplo, en España, CERES.



¿Quién emite los certificados?

Teclados virtuales

- En las transacciones electrónicas de dinero que se llevan a cabo en el comercio electrónico y en el uso de la banca online, hay que extremar las precauciones,
- No solo es información lo que está en juego sino también nuestro dinero.
- Estas paginas suelen incorporar medidas de seguridad adicionales como son la implementación de teclados virtuales en pantalla para introducir los datos [para evitar a los keyloggers].

Cómo usar la banca electrónica

- Usuario y contraseña,
- Coordenadas que figuran en una tarjeta de coordenadas que la entidad entrega al usuario.
- Las precauciones generales son comunes:
 - El canal por el que se accede a la web de la empresa u organismo público es fiable
 - Los métodos de pago son seguros.
 - Tarjeta de crédito,
 - Plataformas de pago, etc.

Transacciones electrónicas de dinero

- 8.- Entra en la web de una empresa de venta de libros y simula la compra de un libro. Captura las imágenes hasta que te ofrezca la forma de pago: ¿Te parece fiable?
- 9.- ¿Dónde compraste por última vez en Internet? ¿Qué medidas de seguridad de las expuestas observaste? (Captura las pantallas dónde se vean) y ¿Qué método de pago utilizaste?
- 10.- Busca en internet el significado de RE-CAPTCHA que utiliza Google, ¿en qué consiste? ¿qué preguntas hace? ¿En qué casos aparecen estas preguntas?, ¿Cuál es la diferencia entre un código BIDI y un QR? ¿Para qué se utilizan? Crea una QR con la letra de una canción y haz que un compañero adivine quién la canta.

Actividades 8 a 10

- A lo largo de esta unidad hemos visto distintas posibilidades para controlar la seguridad en la gestión de los sistemas y aplicaciones informáticas.
- Estas medidas de seguridad se pueden centrar tanto en el **acceso al propio al sistema o aplicación**, como en el **acceso a ciertos recursos o funcionalidades** del mismo.

Otras alternativas a la gestión de identidades

la autenticación

- Es lo que permite **identificar al usuario:**
 - usuario y clave,
 - certificado,
 - etc.

la autorización

- es el mecanismo que decide a qué **recursos puede acceder un usuario** una vez autenticado.

Conceptos: Autentiación y autorización

Existen métodos de autenticación diferentes a los ya vistos de usuario y contraseña:

- Contraseñas de un solo uso,
- Métodos basados en hardware token
- Sistemas biométricos.

Autenticación de usuarios

- Se utilizan normalmente en entornos con elevados requerimientos de seguridad.
- Cada vez que se quiere acceder al sistema se utiliza una contraseña nueva, que tiene un periodo de validez muy corto, con lo cual se minimiza el efecto de acceso por intrusos.
 - Para realizar operaciones en la banca electrónica los bancos suelen enviar a sus usuarios por SMS la contraseña para realizar cada operación.



Contraseñas de un solo uso (OTP, one time password)

- Es un pequeño dispositivo hardware que autentica al usuario que lo lleva y permite, por ejemplo, su acceso a una red.
- Puede tener diferentes formas
 - Tarjeta
 - Llaveró
- Se utiliza lo que se llama autenticación de dos factores:
 - El usuario tiene un número de identificación personal (PIN), que le autentica como propietario del dispositivo.
 - El dispositivo muestra un número que identifica al usuario y le permite el acceso a determinado servicio
- El número de identificación es cambiado frecuentemente para cada usuario.
- Funciona de forma similar a las contraseñas de un solo uso, con la diferencia de que el valor que debe introducirse aparece en una pequeña pantalla en un dispositivo y este cambia regularmente.



Security token, hardware token

- Se trata del uso de sistemas que permiten la autenticación de usuarios mediante características personales inalterables:
 - Huellas digitales
 - Rasgos faciales
 - Iris del ojo
- Requiere la instalación tanto de hardware adicional que capte este tipo de información, como de software específico (algoritmos de reconocimiento) que permita su posterior procesamiento y almacenamiento

Identificación biométrica

- En la operativa habitual de un sistema informático, cada aplicación realiza la autorización de sus usuarios de una manera:
 - Por roles
 - Por Grupos de usuarios
 - ...
- Cuando se intenta centralizar la autenticación y la autorización de todas las aplicaciones en inicio sistema, se recurre a lo que se denomina sistemas de Single Sign-On (SSO).

AutORIZACION DE USUARIOS

- Uno de los principales problemas en las organizaciones es la gestión de identidades.
- En una organización normalmente habrá un sinfín de aplicaciones diferentes que requerirán unos determinados niveles de acceso en cada caso:
 - Todos los empleados deberán tener acceso a la Intranet corporativa para poder ver sus nóminas,
 - Sólo un conjunto determinado de usuarios podrán acceder a las aplicaciones de gestión de contenidos para publicar información nueva en la Intranet.
 - O, solo los directivos tendrán acceso al servidor con los informes del data warehouse.

Single Sign-On (SSO)

- En cada una de estas aplicaciones, lo habitual es que haya un método diferente de gestión de los usuarios:
 - Una base de datos que contiene los coches en venta
 - Una base de datos para almacenar los clientes
- El problema de este enfoque es que ello obliga a los usuarios a introducir sus credenciales cada vez que cambian de aplicación e, incluso, a tener diferentes pares usuario/contraseña en cada una de ellas.

Single Sign-On (SSO)

- Aparte de la incomodidad de este sistema para el usuario, esto genera una serie de problemas adicionales de administración de usuarios:
 - *Si un usuario abandona la organización hay que proceder a borrar su usuario en todos los sistemas, lo cual puede suponer un quebradero de cabeza cuando estos son muy heterogéneos.*
- Lo habitual es tratar de establecer sistemas de SSO, de forma que haya una única base de datos centralizada con todos los usuarios/contraseñas.
 - *El problema es gestionar desde esta base centralizada los diferentes roles que requiere cada aplicación y aquí es donde entra el proceso de autorización.*

Single Sign-On (SSO)

- *Uno de los protocolos mas extendidos de autenticación es Kerberos:*
 - El sistema genera un ticket para el usuario una vez se ha autenticado.
- *Está muy extendido, ya que es el protocolo que utiliza el Active Directory de Windows para la gestión de los usuarios y roles del dominio.*
- *Así, con la combinación de Active Directory + Kerberos es posible establecer la base de un SSO para los servicios básicos proporcionados por la red corporativa de Windows.*
- *Si tenemos aplicaciones de otros fabricantes o bien que han sido desarrolladas a medida, normalmente ya no basta con Active Directory para implementar el SSO:*
 - Será necesario que dichas aplicaciones lleven soporte nativo para integrarse con Active Directory o bien utilizar algún tipo de software que haga de intermediario y proporcione la integración SSO entre Active Directory y las aplicaciones.

Single Sign-On (SSO)

- Actualmente, la mayor parte de las aplicaciones que se desarrollan están pensadas para que el usuario acceda a estas mediante su navegador.
 - Debido a esto, se han generalizado los sistemas de tipo web-SSO, que siguen un sistema semejante al SSO, con la diferencia de que solo **sirven para acceso a aplicaciones vía navegador**, ya que el ticket se intercambia entre el servidor web-SSO y el navegador del cliente, que guarda los datos relativos al ticket en cookies.

Web Single Sign-On (Web-SSO)

- Así, cuando el usuario quiere acceder a alguna aplicación, esta le remite al servidor SSO para que introduzca allí sus credenciales:
 - El SSO mira si se trata de un usuario registrado en la base de datos de usuarios (fase de autenticación) y, a continuación, una vez autenticado, examina si el usuario pertenece al rol necesario para acceder a la aplicación a la que pretende entrar.
 - Si se cumple esta segunda condición (fase de autorización), se genera un ticket, que es el que el usuario le presenta al servidor al que quería acceder.
- Con esto, además de facilitar la administración (en lugar de tener N sistemas de autenticación únicamente hay que gestionar uno centralizado), se evita que el usuario tenga que introducir sus credenciales repetidamente.

Web Single Sign-On (Web-SSO)

- **Web**

www.jasig.org/cast

Pagina web del proyecto CAS de la Universidad de Yale, un sistema de web-SSO bastante extendido. Esta basado en Java y es de código abierto.

Web Single Sign-On (Web-SSO)

- En organizaciones muy grandes, con muchas sedes y departamentos independientes, es posible que **cada sede tenga sus propias aplicaciones** y, a la vez, existan una serie de aplicaciones comunes.
- En estos casos, se intenta establecer relaciones de confianza entre los distintos sistemas de SSO de forma que los usuarios puedan acceder a las aplicaciones a las que estén autorizados con las mismas credenciales en todas las sedes.
- Es lo que se denomina identidad federada.

Identidad federada

- Es la aplicación de la identidad federada a Internet.
 - Si en el caso anterior hablamos de una única organización con diferentes sedes, en este caso lo que tenemos son distintas webs sin relación alguna entre ellas.
- El proyecto OpenID surge para ofrecer la posibilidad de crear una identidad federada entre todos los sitios web que decidan utilizar este sistema.
- Es un sistema abierto y descentralizado:
 - Mantenido por la comunidad de software libre y está disponible para cualquier aplicación o servicio que quiera usarlo

Open ID

- 11.- Busca en Internet ejemplos de sistemas y aplicaciones informáticas donde se utilicen algunas de las alternativas de autenticación y autorización vistas.
- 12.-¿Qué sistemas de identificación biométrica utiliza el DNI electrónico?
- 13.-¿Qué son los sistemas SSO?
- 14.- ¿Qué diferencia hay entre autenticación y autorización?

Actividades 11 a 14