# GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

## Capítulo 7.

## Administración del control de accesos. (1ª Parte)

José Pablo Hernández

## ¿Qué es un control de accesos?

Un control de accesos es un dispositivo que tiene por objeto impedir el libre acceso del público en general a diversas áreas que denominaremos protegidas.

Por lo tanto lo primero que se debe identificar, para justificar la instalación de un control de accesos, es la existencia de elementos que se desean proteger.

El control de acceso es el proceso por el cual se autoriza a usuarios, grupos y equipos obtener acceso a los objetos de la red mediante permisos, derechos de usuario y auditoría de objetos.

¿Qué es un control de accesos?

Para comprender y administrar el control de acceso, debe comprender la relación entre lo siguiente:

- Objetos (archivos, impresoras y otros recursos)
- Tokens de acceso
- Listas de control de acceso (ACL) y entradas de control de acceso (ACE)
- Sujetos (usuarios o aplicaciones)
- El sistema operativo
- Permisos
- Derechos y privilegios de usuario

¿Qué es un control de accesos?

Para que un sujeto pueda tener acceso a un objeto, debe identificarse en el subsistema de seguridad del sistema operativo.

Esta identidad está incluida en un token de acceso que se vuelve a crear cada vez que un sujeto inicia una sesión.

Antes de permitir que el sujeto tenga acceso a un objeto, el sistema operativo determina si el token de acceso del sujeto está autorizado para tener acceso al objeto y completar la tarea deseada.

Para ello, compara la información del token de acceso con las entradas de control de acceso (ACE) del objeto.

¿Qué es un control de accesos?

Las ACE pueden permitir o denegar distintos comportamientos según el tipo de objeto.

Por ejemplo, las opciones de un archivo pueden ser Leer, Escribir y Ejecutar.

En una impresora, las ACE disponibles pueden ser Imprimir, Administrar impresoras y Administrar documentos.

¿Qué es un control de accesos?

Las ACE individuales de un objeto se combinan en una lista de control de acceso (ACL).

El subsistema de seguridad comprueba si la ACL del objeto incluye ACE relacionadas con el usuario y los grupos a los que éste pertenece.

Revisa cada ACE hasta que encuentra una que permite o deniega el acceso al usuario o uno de sus grupos, o bien hasta que no queda ninguna ACE por comprobar.

Si llega al final de la ACL y no ha encontrado ninguna ACE en la que se permita o se deniegue explícitamente el acceso deseado, el subsistema de seguridad deniega el acceso al objeto.

¿Qué es un control de accesos?

Permisos

Los permisos definen el tipo de acceso concedido al usuario o grupo para un objeto o una propiedad de objeto.

Por ejemplo, al grupo Finanzas se le pueden conceder los permisos de lectura y escritura para el archivo denominado Payroll.dat.

Los permisos se pueden conceder a cualquier usuario, grupo o equipo.

Es recomendable asignar permisos a grupos, ya que esto mejora el rendimiento del sistema cuando se comprueba el acceso a un objeto.

¿Qué es un control de accesos?

Permisos

Los permisos adjuntos a un objeto dependerán del tipo de objeto.

Por ejemplo, los permisos que se pueden adjuntar a un archivo son diferentes de los que se pueden adjuntar a una clave del Registro.

Sin embargo, algunos permisos son comunes a la mayoría de los tipos de objeto.

Los permisos comunes son:

- Leer
- Modificar
- Cambiar propietario
- Eliminar

¿Qué es un control de accesos?

Permisos

Cuando se establecen permisos, se especifica el nivel de acceso de los grupos y usuarios.

Por ejemplo, puede permitir a un usuario leer el contenido de un archivo, dejar a otro usuario realizar cambios en el archivo y evitar a los demás usuarios el acceso al archivo.

Puede establecer permisos similares en impresoras para que determinados usuarios puedan configurarlas y otros usuarios sólo puedan imprimir.

¿Qué es un control de accesos?

Propiedad de objetos

Cuando se crea un objeto, se le asigna un propietario.

De forma predeterminada, el propietario es el creador del objeto.

Sean cuales sean los permisos que se definan en un objeto, el propietario del objeto siempre puede cambiarlos.

¿Qué es un control de accesos?

Herencia de permisos

La herencia permite a los administradores asignar y administrar permisos fácilmente.

Esta característica hace que los objetos de un contenedor hereden automáticamente todos los permisos heredables de ese contenedor.

Por ejemplo, cuando se crean archivos en una carpeta, heredarán los permisos de la carpeta.

Sólo se heredarán los permisos marcados para ello.

¿Qué es un control de accesos?

Derechos y privilegios de usuario

Los derechos de usuario conceden determinados privilegios y derechos de inicio de sesión a los usuarios y grupos del entorno de computación.

Los administradores pueden asignar derechos específicos a las cuentas de grupo o a cuentas de usuario individuales.

Estos derechos autorizan a los usuarios a realizar acciones específicas, como iniciar una sesión en un sistema de forma interactiva o realizar copias de seguridad de archivos y directorios.

¿Qué es un control de accesos?

Derechos y privilegios de usuario

Los derechos de usuario conceden determinados privilegios y derechos de inicio de sesión a los usuarios y grupos del entorno de computación.

Los administradores pueden asignar derechos específicos a las cuentas de grupo o a cuentas de usuario individuales.

Estos derechos autorizan a los usuarios a realizar acciones específicas, como iniciar una sesión en un sistema de forma interactiva o realizar copias de seguridad de archivos y directorios.

¿Qué es un control de accesos?

Auditoría de objetos

Los derechos de administrador permiten auditar el acceso correcto o incorrecto de los usuarios a los objetos.

(En Windows 2008 primero debe habilitar la directiva de auditoría seleccionando **Auditar el acceso a objetos** en **Directiva local\Directiva de auditoría\Directivas locales** del complemento Directiva de seguridad local. A continuación, podrá ver estos eventos relacionados con la seguridad en el registro de seguridad del visor de eventos.)

Aspectos básicos de seguridad.

Para todos los protocolos, contraseñas y claves, la seguridad resuelve tres conceptos básicos:

**Autenticación**: Confirmación de la identidad de una persona o entidad antes de permitir el acceso a un recurso.

**Protección de datos:** Cómo asegurar la privacidad e integridad de los datos trasmitidos o almacenados.

**Control de acceso:** Restricción del acceso a los datos y recursos a los usuarios con privilegios.

Aspectos básicos de seguridad. **Autenticación.**

**Autenticación** describe el proceso en el cual una persona o entidad se identifica a sí mismo ante una segunda parte.

En términos generales, esto puede significar mostrar el carné de identidad a un cajero de banco o insertar una tarjeta de crédito en un cajero automático e introducir un PiN.

En un lenguaje de computadoras, autenticación es un poco más deductivo.

A diferencia del cajero del banco, que posee el lujo del contacto personal, casi todos los escenarios de autenticación relacionados con computadoras son virtuales.

Aspectos básicos de seguridad. **Autenticación.**

**Prueba de identidad**

Normalmente, la prueba de identidad viene en forma de un secreto compartido entre el demandante y el autenticador: una contraseña, un PIN o una clave de cifrado.

La palabra principal es «secreto».

La clave del proceso completo de autenticación es la creencia del autenticador de que el demandante -y sólo el demandante- posee ese secreto.

Cuando esto deja de ser verdad, el sistema, en algún u otro grado, está comprometido.

Aspectos básicos de seguridad. **Autenticación.**

**Prueba de identidad**

Dependiendo del protocolo que se utilice, el secreto compartido se comunica al autenticador, quien entonces concede o deniega el acceso.

Los protocolos seguros protegen el secreto en tránsito;
en esquemas mis elaborados el secreto no se envía del todo.

La tecnología de clave pública usa una pareja de claves de cifrado -una clave privada que nunca se expone y una clave pública que puede estar diseminada-.

Existen una serie de protocolos para probar la posesión de las credenciales de identificación.

Aspectos básicos de seguridad. **Autenticación.**

**Protocolos de autenticación**

Claramente, la eficacia de un proceso de autenticación y la seguridad del secreto dependen del protocolo que se use.

Protocolos usados:

- Kerberos versión ***5***
- Protocolo de autenticación extensible **(EAP)**
- Protocolo de autenticación de contraseña **(PAP)**
- Protocolo de autenticación desafío mutuo Microsoft. versión 2 (**MS-CHAP v2**)
- **SSL/TLS**

Aspectos básicos de seguridad. **Autenticación.**

**Protocolos de autenticación**

**Autenticación mutua**

La autenticación no necesariamente tiene que ser de un único sentido.

Muchas veces el demandante querría probar la identidad del host de autenticación.

Por ejemplo, cuando se crea un vínculo seguro a un directorio restringido en el que se van a intercambiar datos confidenciales, son importantes tanto la identidad del cliente como la del servidor.

Protocolos como SSL/TLS permiten la autenticación mutua entre cliente y servidor.

Aspectos básicos de seguridad. **Autenticación.**

Existen tres métodos de autenticación:

**Basados en algo conocido**: contraseñas, frases de paso, etc.

**Basados en algo poseído**: tarjeta de identidad, tarjeta inteligente (*smartcard*), dispositivo usb (*token*), etc.

**Basados característica físicas del usuario**: verificación de voz, escritura, huellas, patrones oculares, etc.

Aspectos básicos de seguridad. **Protección de datos.**

Los esquemas de autenticación que protegen las contraseñas cuando atraviesan una red no segura son cruciales para mantener un sistema seguro; igual de importantes son los datos enviados cuando se ha  iniciado una sesión.

Si es información propiedad de la compañía o si es la tarjeta de crédito de una persona, el tema es el mismo: impedir la lectura de la información de red por parte de personas no autorizadas e impedir que se modifique.

Aspectos básicos de seguridad. **Protección de datos.**

Confidencialidad de los datos.

La privacidad de los datos, sean un mensaje de correo electrónico, las entradas en una página Web o distintos paquetes IP, se pone en peligro una vez que la información se trasmite a través de líneas de comunicación no seguras, como Internet.

Usando algoritmos y claves de cifrado, se puede proteger la privacidad de los datos.

Sin las claves correspondientes para descifrar, los receptores no deseados que intercepten la trasmisión no recibirán más que basura cifrada.

Aspectos básicos de seguridad. **Protección de datos.**

Confidencialidad de los datos.

La resistencia del cifrado también depende del algoritmo usado y la longitud de la clave.

Con potencia de computación suficiente, cualquier clave de cifrado se puede romper.

Aspectos básicos de seguridad. **Protección de datos.**

Confidencialidad de los datos.

Normalmente, el grueso de los datos se cifra usando una algoritmo de bloque de cifras (también conocidos como algoritmos simétricos) y una clave.

La resistencia de este método reside en las cadenas de bloques de cifras (CBC).

Cifrando un bloque cada vez, la salida de un bloque se usa como entrada para el siguiente.

De esta forma, los patrones repetidos de datos no producen los mismos datos cifrados.

La entrada al primer bloque es un número aleatorio llamado vector de inicialización (IV).

El IV asegura que cada vez que se cifra un mensaje, el resultado producido es único.

Aspectos básicos de seguridad. **Protección de datos.**

Confidencialidad de los datos.

Para la confidencialidad de los datos trasmitidos a nivel de red, se puede emplear el Protocolo de Internet seguro (IPSec).

IPSec cifra los paquetes de TCP/IP antes de su trasmisión y los descifra después de su recepción.

Aspectos básicos de seguridad. **Protección de datos.**

Confidencialidad de los datos.

La confidencialidad de los datos almacenados también es un problema.

Aunque el acceso a los archivos almacenados se puede restringir a determinados usuario mediante los permisos de archivo, los intrusos que consiguen acceso al disco duro pueden cambiar esos permisos.

Aspectos básicos de seguridad. **Protección de datos.**

Integridad de los datos.

Aunque el cifrado puede garantizar la confidencialidad de un archivo, no puede garantizar la integridad de los datos del archivo, es decir, que no se ha modificado  el archivo.

La firma digital de un archivo, módulo o cualquier otro componente software, es como la firma de un contrato en papel.

El firmante es responsable de lo que firma.

Quienquiera que vea posteriormente el documento y la firma puede decir quién lo firmó.

Aspectos básicos de seguridad. **Protección de datos.**

Integridad de los datos.

Sin embargo. las firmas digitales ofrecen una gran cantidad de seguridad por debajo de esto.

Una firma digital se genera fragmentando el documento y cifrándolo con la clave privada de cifrado del firmante.

Este procedimiento produce una firma que está repartida de forma cifrada tanto por el firmante como por el contenido del documento.

El cambio del contenido rompe la firma.

Aspectos básicos de seguridad. **Protección de datos.**

Integridad de los datos.

Tras la verificación, la firma digital se descifra con la clave pública del firmante.

Los fragmentos resultantes se comparan con los fragmentos recién calculados del mensaje.

Este proceso prueba de forma innegable que el firmante firmó este mensaje, ya que su clave se usó para verificar la firma; además, verifica que los contenidos del documento no se han cambiado, ya que los fragmentos cifrados coinciden con los fragmentos recién calculados.

Aspectos básicos de seguridad. **Protección de datos.**

Integridad de los datos.

La firma digital tiene dos propósitos significativos.

Primero, garantizar la integridad de los datos almacenados de forma local o que pasen a través de la red.

Segundo, la autenticación de módulo o cualquier otro componente software obtenido a partir de fuentes en las que no se confía, como Internet.

La validación de la firma de un módulo verifica que el software no ha sido alterado y que lo firmó un creador de software de confianza.

Aspectos básicos de seguridad. **Protección de datos.**

Integridad de los datos.

Los dos algoritmos de firma digital más conocidos son el RSA y el Algoritmo de firma digital (DSA).

Las firmas DSA tienen 40 bytes de longitud, mientras que la longitud de las firmas RSA dependen del tamaño de la clave.

Un par de claves, consistente en una clave pública y una clave privada, con clave pública de 128 bytes suele producir una firma de 128 bytes.

Aspectos básicos de seguridad. **Control de acceso.**

La autenticación es la primera capa de seguridad en la protección de objetos y recursos de red.

La segunda capa es el control de acceso, es decir, el control de a qué recursos se puede acceder, por parte de quién y con qué permisos.

Un usuario autenticado no necesariamente tiene la autorización para acceder a todos los archivos, impresoras y claves del registro.

El control de acceso lo impone el administrador para cada tipo de objeto, pero es tarea del propietario del objeto determinar qué restricciones de control de acceso imponer.

Aspectos básicos de seguridad. **Control de acceso.**

El acceso se controla mediante la asignación de derechos a usuarios y asignando permisos para los objetos.

Los permisos especifican qué usuarios pueden acceder a un determinado objeto y qué tipo de acceso está permitido.

Por ejemplo, el propietario de una hoja de cálculo trimestral de una empresa financiera puede fijar permisos que permitan acceso de lectura/escritura a la dirección de la empresa, permitir acceso sólo lectura a todos los miembros de la empresa y denegar el acceso al resto.

Aspectos básicos de seguridad. **Control de acceso.**

Los grupos de usuarios tienen sus propios derechos y se puede especificar cuándo se conceden los permisos del objeto.

En el ejemplo anterior, establecer permisos de sólo lectura para todos en la empresa probablemente signifique asignar derechos de grupo, no asignar los derechos de usuario de forma individual.

Aspectos básicos de seguridad. **Control de acceso.**

Se pueden asignar permisos de forma explícita para un objeto o para facilitar la administración, o también se pueden heredar de los objetos padres.

Sin embargo, el detalle del control de acceso no se detiene en los objetos.

Se pueden asignar permisos incluso para atributos de objeto, permitiendo acceso a algunos campos como la dirección de correo electrónico de una cuenta de usuario, mientras se deniega el acceso a otros campos, como el número de teléfono del usuario.

Aspectos básicos de seguridad. **Control de acceso.**

Los permisos estándar de objeto comprenden los siguientes:

- Lectura del objeto.
- Modificación del objeto.
- Eliminación del objeto.
- Lectura de los permisos del objeto.
- Modificación de los permisos del objeto.
- Cambio del propietario del objeto.

Aspectos básicos de seguridad. **Infraestructura de clave pública.**

En los últimos años, las infraestructuras de clave pública (PKI) han tomado ímpetu en los sectores comercial y gubernamental.

Basado en la tecnología de clave pública, una PKI describe un sistema de generación y administración de certificado de clave pública, incluyendo su distribución y revocación.

Aspectos básicos de seguridad. **Infraestructura de clave pública.**

Una de las ventajas distintivas del uso de los certificados de clave pública para la autenticación es que los servidores ya no necesitan almacenar y mantener una lista de contraseñas para los usuarios individuales.

Debido a que la identificación está basada en la relación de confianza con los CA, los servidores sólo necesitan confiar en la autoridad que expide el certificado del demandante.

Una vez determinada la cadena de confianza y verificado el certificado, se establece la autenticación.

Aspectos básicos de seguridad. Directivas de contraseña.

Usar contraseñas complejas y cambiarlas regularmente reduce la probabilidad de que un ataque de contraseñas tenga éxito.

La configuración de la Directiva de Contraseñas controla la complejidad y la vida útil de las contraseñas.

La creación de requisitos estrictos acerca de la longitud y complejidad de las contraseñas no implica necesariamente que los usuarios y administradores usen contraseñas sólidas.

Al activar las directivas de contraseñas, los usuarios del sistema pueden cumplir los requisitos de complejidad técnica de la contraseña definidos por el sistema, pero se necesita una fuerte directiva de seguridad corporativa adicional para erradicar los malos hábitos en cuanto a las contraseñas.

Por ejemplo, Breakfast! puede cumplir todos los requisitos de complejidad de una contraseña, pero no es muy difícil de descifrar.

Aspectos básicos de seguridad. Directivas de contraseña.

Conociendo a la persona que ha creado la contraseña, usted puede ser capaz de adivinarla basándose en su comida, coche o película preferidos.

Una de las estrategias de un programa de seguridad corporativa para educar a sus usuarios en la elección de contraseñas sólidas es crear un cartel que describa las contraseñas débiles y colocarlo en las áreas comunes, cerca de la máquina de bebidas o de la fotocopiadora.

Aspectos básicos de seguridad. Directivas de contraseña.

Cada empresa debe establecer unas pautas para la creación de contraseñas adecuadas que incluyan:

- Evitar el uso de palabras que figuren en el diccionario, palabras con errores ortográficos comunes o ingeniosos y palabras extranjeras.
- Evitar la adición de un dígito a la contraseña.
- Evitar colocar números al principio o al final de la contraseña.
- Evitar usar contraseñas que otros puedan adivinar fácilmente mirando su escritorio (tales como nombres de mascotas, equipos deportivos o parientes).
- Evitar el uso de palabras de la cultura popular.
- Evitar pensar en contraseñas que sean palabras propiamente dichas: piense en códigos secretos.
- Obligar a usar contraseñas que deban teclearse con las dos manos sobre el teclado.
- Obligar a usar letras mayúsculas y minúsculas, números y símbolos en todas las contraseñas.
- Obligar a usar caracteres que sólo puedan escribirse pulsando la tecla Alt.

Aspectos básicos de seguridad. Directivas de contraseña.

El parámetro **Forzar el historial de contraseñas** determina el número de contraseñas Únicas nuevas que deben asociarse a la cuenta de un usuario antes de que sea posible reutilizar una contraseña antigua.

Debe fijarse el valor entre 0 y 24 contraseñas.

Este parámetro de la directiva permite a los administradores incrementar la seguridad, garantizando que no se reutilizan continuamente las contraseñas antiguas.

Para mantener la efectividad del historial de contraseñas, configure también la Vida mínima de la contraseña para evitar que las contraseñas sean cambiadas inmediatamente.

Así, es difícil que los usuarios reutilicen las contraseñas, sea accidental o conscientemente.

Aspectos básicos de seguridad. Directivas de contraseña.

El parámetro **Vida mínima de la contraseña** determina el número de días que debe usarse una contraseña antes de que el usuario la cambie.

El rango de valores de este parámetro va desde 0 hasta 999 días. Fijarlo en 0 le permite cambiar la contraseña inmediatamente.

El parámetro Vida mínima de la contraseña debe ser menor que el parámetro Vida máxima de la contraseña, a menos que la Vida máxima de la contraseña se ajuste a 0, lo cual indicaría que las contraseñas nunca caducan.

En este caso, la Vida mínima de la contraseña puede tomar cualquier valor entre 0 y 999.

Aspectos básicos de seguridad. Directivas de contraseña.

Ajuste la Vida mínima de la contraseña a un valor mayor que 0 si quiere que Forzar el historial de contraseñas sea eficaz.

Sin una vida mínima de la contraseña, los usuarios pueden rotar repetidamente sus contraseñas hasta llegar a una antigua favorita.

Cambie este valor a 2 días porque, cuando el valor se usa en conjunción con un valor pequeño similar para el parámetro Forzar el historial de contraseñas, la restricción disuade a los usuarios de reciclar una y otra vez la misma contraseña.

Si la Vida mínima de la contraseña se fija en un día y Forzar el historial de contraseñas se configura para 2 contraseñas, los usuarios sólo tendrían que esperar dos días enteros antes de cambiar las contraseñas.

Aspectos básicos de seguridad. Directivas de contraseña.

El parámetro **Longitud mínima de la contraseña** garantiza que las contraseñas tengan como mínimo un cierto número de caracteres.

Las contraseñas largas (ocho o más caracteres) suelen ser más sólidas que las cortas.

Con esta directiva, los usuarios no pueden usar contraseñas en blanco y se ven obligados a crear contraseñas que tengan un determinado número de caracteres.

Aspectos básicos de seguridad. Directivas de contraseña.

Se recomienda la contraseña de ocho caracteres porque es lo suficientemente larga para ofrecer un cierto nivel de seguridad y lo bastante corta para que los usuarios la recuerden con facilidad.

Este parámetro ofrece una buena defensa contra los ataques comunes con diccionario y fuerza bruta.

Aspectos básicos de seguridad. Directivas de contraseña.

Un ataque con diccionario es un método para obtener una contraseña a través de pruebas y errores en el cual el atacante usa todos los elementos de una lista de palabras.

Un ataque por fuerza bruta es un método de obtener una contraseña u otro texto encriptado probando todos los valores posibles.

La viabilidad de un ataque por la fuerza bruta depende de la longitud de la contraseña, el tamaño del conjunto de caracteres potenciales y la capacidad informática de la que disponga el atacante.

Aspectos básicos de seguridad. Directivas de contraseña.

La opción **La contraseña debe cumplir todos los requisitos de complejidad** comprueba todas las nuevas contraseñas para garantizar que cumplen los requisitos de una contraseña sólida.

Los requisitos de complejidad se fuerzan cuando se crean las contraseñas.

Se puede crear una contraseña de 20 o más caracteres que resulte más fácil de recordar para el usuario (y más segura) que una de ocho caracteres.

La siguiente contraseña de 27 caracteres: *I love cheap tacos for $.99*, por ejemplo. Este tipo de contraseña, en realidad una frase, puede ser más fácil de recordar que una más corta como *FQ55wOrd*.

Aspectos básicos de seguridad. Directivas de contraseña.

Este valor recomendado, combinado con una Longitud mínima de la contraseña de 8, incluye letras mayúsculas y minúsculas y números del teclado, lo cual incrementa el número de caracteres de 26 a 62 caracteres.

Una contraseña de ocho caracteres tendrá entonces 2.18 x 1014 combinaciones posibles.

A razón de 1.000.000 de intentos por segundo, se tardaría 6,9 años en comprobar todas las permutaciones posibles.

El uso conjunto de estos parámetros hace muy difícil un ataque por la fuerza bruta.

Aspectos básicos de seguridad. Directiva de bloqueo de cuentas.

La **Directiva de Bloqueo de Cuentas** es una característica de seguridad que bloquea la cuenta de un usuario después de un número de intentos de inicio de sesión fallidos durante un cierto período de tiempo.

El usuario no puede iniciar sesión en una cuenta bloqueada y el software servidor puede configurarse para responder a este tipo de posible ataque deshabilitando la cuenta para un número predeterminado de intentos fallidos de iniciar una sesión.