



SEGURIDAD DE LA

INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

Procedimiento general para la revisión de cuentas de usuario en Active Directory

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 1.0 | **Categoría** | Procedimiento |
| **Última actualización** | 30/07/2018 | **Estado** |  |

# Objetivo

Establecer los procedimientos generales para la revisión de las cuentas de usuario en un controlador de dominio Active Directory, con el fin de prevenir y mitigar accesos no autorizados por medio de este sistema de control.

# Alcance

El procedimiento presentado va orientado única y exclusivamente a realizar las acciones de revisión de todas las cuentas de usuario que están almacenadas en el controlador de dominio Active Directory de la organización. A través la realización de una revisión al menos trimestral, se puede validar la integridad de los atributos y roles de los usuarios y en caso de ser necesario realizar cambios y depuraciones en el sistema.

# Responsabilidades

**Responsable de seguridad de la información** debe velar por el cumplimiento de este procedimiento en la periodicidad que corresponda.

**Personal de seguridad de la información** debe ser el responsable de la ejecución de procedimiento en la periodicidad que corresponda y realizar las adecuaciones en caso de obtener alguna desviación.

**Personal de RRHH** debe poder suministrar información relevante del personal en caso que el área de seguridad de la información lo requiera, como ser fechas de alta y baja de personal.

# Descripción

El procedimiento aquí descrito solo es la base para realizar las acciones que permita poder cumplir con los puntos del marco de Ciberseguridad de AGESIC de la categoría Protección y Subcategoría PR.CA-1 del requisito CA-2 revisión de los accesos lógicos.

Los comandos descritos pueden ser utilizados para realizar la revisión de los usuarios creados en Active Directory en ambientes Windows Server 2008 y superiores. Estos comandos deben ejecutarse en una sesión con privilegios de administrador de dominio.

Los comandos son los siguientes:

1. **Listado de usuarios habilitados**

**Comando:**

csvde -f C:\habilitados.csv  -r "(&(objectcategory=person)(objectclass=user)(!useraccountcontrol:1.2.840.113556.1.4.803:=2))"

1. **Listado de usuarios deshabilitados**

**Comando:**

csvde -f C:\deshabilitado.csv  -r "(&(objectcategory=person)(objectclass=user)(useraccountcontrol:1.2.840.113556.1.4.803:=2))"

**Nota:** Algunos de los campos de fecha, como es el caso de lastLogon, se exportan en un formato que requiere conversión. Se incluye fórmula para convertir estos campos:

**Fórmula:** =X#/(8,64\*10^11) – 109205

Donde, “X#” es la celda que incluye el valor a convertir.

**Ejemplo:** =U3/(8,64\*10^11) - 109205

Los campos conteniendo el resultado de la fórmula deben ser establecidos como formato Fecha para que se visualicen correctamente.

1. **Listado de usuarios habilitados a los que no les expira la contraseña**

**Comando:**

dsquery \* -filter "(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))" -attr name -limit 0 > C:\usuariosnoexpirapwd.txt

1. **Listado de usuarios habilitados que no inician sesión en un tiempo dado**

**Comando:**

dsquery user –inactive <semanas> -limit 0 > C:\usuarioshabilitados-inactivos.txt

**Donde**, “semanas” es el parámetro a modificar por un valor numérico mayor a 0, correspondiente a la cantidad de semanas transcurridas desde el último inicio de sesión. Se recomienda un valor entre 4 y 6.

**Ejemplo:** dsquery user –inactive 4 –limit 0 > C:\usuarioshabilitados-inactivos.txt

1. **Listado de usuarios bloqueados por exceso de intentos erróneos de inicio de sesión**

**Comando:**

csvde -f C:\lockedout.csv -r "(&(&(&(&(&(&(&(objectCategory=person)(objectClass=user)(lockoutTime:1.2.840.113556.1.4.804:=4294967295))))))))"

1. **Listado de usuarios que no cambian su contraseña**

**Comando:**

dsquery user -stalepwd  X > C:\usuariosnocambianclave.txt

Donde, “X” es el parámetro a modificar, siendo numérico mayor a 0 y correspondiente a la cantidad de días transcurridos desde el último cambio de contraseña. Se recomienda usar el valor estipulado en la política del dominio para validar este punto.

**Ejemplo:** dsquery user -stalepwd 60 > C:\usuariosnocambianclave.txt

1. **Listado de usuarios que no han iniciado sesión**

**Comando:**

dsquery \* -filter ("&(objectCategory=person)(objectClass=user)(!userAccountControl:1.2.840.113556.1.4.803:=2)(!lastLogonTimeStamp>=1))" -attr name –limit 0 > C:\usuariossininicio.txt

**Nota:** La salida de los comandos se redirecciona con “>” o con la opción “-f”. La ruta de los archivos o su nombre pueden ser modificados acorde a las necesidades. El formato de los archivos exportados con la opción “–f” es CSV, y los redireccionados con “>” es texto plano.

**Procedimiento detallado**

1. Conectarse al controlador de dominio mediante Escritorio Remoto con credenciales de administrador de dominio.
2. Abrir **símbolo de sistema** y ejecutarlo como administrador.



1. Ajustar cada de los comandos uno a uno a las necesidades de la organización y pegarlos en el símbolo de sistema. Presionar Enter y esperar la salida al archivo definido.



1. Los archivos obtenidos serán guardados en formatos .CSV y .TXT. Los archivos en formato .CSV, deben ser importados en una planilla Excel vacía. Para ello, abrir Excel y en una planilla vacía, ir a Datos y seleccionar Desde Texto en la sección Obtener datos externos. Buscar el archivo en la ubicación guardada y seleccionarlo. El tipo de archivo es Delimitado, se debe marcar que los datos contienen encabezados y presionar Siguiente. Como delimitador, seleccionar Coma o Punto y Coma (dependiendo de la configuración del equipo) y en calificador de texto seleccionar la comilla doble y presionar Finalizar.

Los archivos pueden ser abiertos en OpenOffice que permite realizar este procedimiento al abrir los archivos.

1. Guarde en lugar seguro todos los archivos generados.
2. Trabaje con una copia de todos los archivos.
3. Solicite al área de Recursos Humanos un listado del personal con las altas, bajas y personal de licencia por un período no mayor al auditado.
4. Ejecutar los siguientes controles sobre los archivos:

**Listado de usuarios habilitados:**

* Verificar que el nombre y apellido en los campos First Name y Last Name coincidan.
* Verificar que el campo whenCreated esté relacionado con el tiempo de ingreso del usuario a la organización.
* Verificar fecha del último inicio de sesión en el campo lastLogon.
* Verificar fecha del último cambio de clave pwdLastSet.

Es importante tener identificados los usuarios que tengan rol administrador dentro del dominio para verificar que esta situación sea correcta.

**Listado de usuarios deshabilitados**

* Verificar que el nombre y apellido en los campos First Name y Last Name coincidan.
* Verificar que el campo whenChanged esté relacionado con el tiempo de culminación de actividades del usuario en la organización en caso de haber sido una baja.
* Verificar fecha del último cierre de sesión en el campo lastLogoff.
* Verificar fecha del último inicio de sesión en el campo lastLogon.

**Nota:** Contrastar las fechas exportadas contra la información suministrada desde Recursos Humanos.

Es importante tener identificados los usuarios que tienen privilegios de administrador en el dominio para verificar el estado y constatar que las políticas establecidas en el dominio y la política de seguridad de la información se estén ejecutando de forma correcta sobre cada usuario.

**Listado de usuarios que no les expira la contraseña**

* Verificar si los usuarios listados en el archivo (.TXT) son correctos.
* Se debe contar con una lista de los usuarios de sistema y servicios para excluirlos de la revisión.
* Aquellos usuarios que no deban poseer el atributo de No expiración activado y lo tengan activado, deben ser verificados.

**Listado de usuarios habilitados que no inician sesión en un tiempo dado**

* Verificar los usuarios listados en el archivo (.TXT).
* Se debe contar con una lista de los usuarios de sistemas para excluirlos de la revisión.
* Aquellos usuarios que están inactivos se deben bloquear y verificar si los mismos deben ser eliminados del dominio.

**Listado de usuarios bloqueados por exceso de intentos erróneos de inicio de sesión**

* Verificar los usuarios listados en el archivo (.CSV).
* Se debe contar con una lista de usuarios administradores para validar que no se esté intentando un ataque contra esas cuentas.
* El control validará si en un periodo de tiempo se producen una cantidad significativa de bloqueos para el inicio de su sesión.
* Verificar fecha de la última colocación de clave errónea en el campo badPasswordTime.
* Solicitar ayuda CERTuy si se considera que no pueden validar desde que punto de la red se pueden estar generando los intentos de inicio de sesión con el fin de poder identificar el origen.

**Listado de usuarios que no cambian su contraseña**

* Verificar usuarios listados en el archivo (.TXT).
* Se debe contar con una lista de los usuarios de los sistemas y servicios para excluirlos de la revisión.
* Aquellos usuarios que están activos se deben verificar que no tengan habilitada la opción de no expiración de contraseña, de ser así se debe modificar este parámetro y marcar la opción cambiar contraseña en el siguiente inicio de sesión.

**Listado de usuarios que no han iniciado sesión**

* Verificar los usuarios listados en el archivo (.TXT).
* Se debe contar con una lista de los usuarios de los sistemas y servicios para excluirlos de la revisión.
* Aquellos usuarios que no han iniciado de sesión deben ser verificados con Recursos Humanos.

# Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en el procedimiento e incumpliendo con la política de seguridad de la información, la Dirección del Organismo podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

# Historial de revisiones

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

