



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 Samba

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 4.0 | **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 Samba, 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 Samba de la organización. A través de 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 es la base para realizar las acciones que permitan dar cumplimiento a los puntos del marco de Ciberseguridad de AGESIC de la categoría Protección, Subcategoría PR.CA-1, requisito CA-2 - Revisión de los accesos lógicos.

Los comandos aquí descritos pueden ser utilizados para realizar la revisión de los usuarios en un entorno Samba. Estos comandos o rutas de acceso deben ejecutarse en una sesión con privilegios de administrador.

Los comandos son los siguientes:

1. **Listar el archivo de configuración de Samba**

Para ello se necesita el archivo “smb.conf” de configuración de Samba, que se puede encontrar en alguna de las siguientes ubicaciones dependiendo de la instalación:

* usr/samba/lib
* /usr/local/samba/lib
* /etc/samba
1. **Listar usuarios del servidor de Samba**

El archivo “smbusers” se puede encontrar en general en la siguiente ubicación: “/etc/samba/smbusers”.

Se debe validar el tipo de base de datos en el archivo “smb.conf”. La siguiente sección considera los diversos tipos de base de datos, se deben seguir los pasos de la base de datos instalada.

**Comandos:**

Base de datos: SMBPASSWD

Para las siguientes PASSDB (TDBSAM, LDAPSAM, MYSQLSAM, XMLSAM, ETC).

* pdbedit -L -w >> passwd.txt (lista los usuarios en formato "smbpasswd").
* pdbedit -L -v >> passwdDetallado.txt (lista de usuarios detallada).
1. **Diagnóstico del servicio del controlador de dominio**

El archivo se puede encontrar en las siguientes ubicaciones:

* testparm -s /etc/samba/smb.conf >> testparm\_salida.txt
* testparm -diagnostics > diagnosticos.txt

**Procedimiento detallado**

1. Guarde en lugar seguro todos los archivos generados.
2. Trabaje con una copia de todos los archivos.
3. Los archivos obtenidos serán guardados en formato .TXT. El archivo “passwd.txt”, debe ser importado en una planilla Excel vacía. Para ello, abrir Excel y en una planilla vacía, ir a Datos – Obtener datos externos y seleccionar Desde Texto. Buscar el archivo en la ubicación guardada y seleccionarlo. El tipo de archivo es Delimitado y presionar Siguiente. Como delimitador, seleccionar Otros y en la casilla colocar “:” y en calificador de texto seleccionar la comilla doble y presionar Finalizar.
4. 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.
5. Una vez que vaya a trabajar “passwd” ya vaciado en la hoja de Excel, se le recomienda colocarle nombre a cada una de las columnas. Suponiendo que escogió la **(=hoja1!$A$1)** de su hoja de Excel, debe seleccionar la fila A1 y con el botón derecho del ratón indicarle insertar, para que los valores ahora se reflejen en la fila A2. Los nombres sugeridos para colocar en cada columna son:
* **Columna A1:** UserName
* **Columna B1:** UserID
* **Columna C1:** LAN Manager Password Hash
* **Columna D1:** NT Password Hash
* **Columna E1:** Account Flags
* **Columna F1:** Last Change Time (LCT)
1. Ahora antes de comenzar el control debemos realizar una serie de pasos en la hoja de Excel, para determinar los estados de los usuarios:

De la Columna G a la Q se van a colocar los siguientes nombres:

**Columna G1:** Fecha Último Cambio, donde se reflejará la fecha del último cambio del password realizado por el usuario.

* **Formula:** = FECHA(1970;1;1)+(HEX.A.DEC(EXTRAE(**F2**;5;10))/86400)
* La configuración del formato de la celda es “Fecha”, Ej. “\*31/5/2018”.

**Columna H1:** Días Ultimo Cambio, donde se podrá observar la cantidad de días en el que el usuario no ha realizado cambio de contraseña. En la primer parte de la fórmula, se deben sustituir los valores <diaArchivo>, <mesArchivo>, <añoArchivo> por la fecha en la que el archivo fue copiado del sistema.

* **Formula:** =FECHA(<añoArchivo>;<mesArchivo>;<diaArchivo>)-**G2**
* La configuración del formato de la celda es “Número”, Ej. “-1234”.

**Columna I1:** Infringe política, donde X es la vida máxima de la contraseña en días y se validara si los usuarios exceden en el parámetro configurado en la política. En caso de no saber qué política está establecida, puede ejecutar el siguiente comando:

* sudo pdbedit -P "maximum password age"
* **Formula:** =SI(**H2**>**X**;"Sí";"No")
* La configuración del formato de la celda es “General”.

**Columna J1:** Nunca Cambió Contraseña, donde se determinará si el usuario cambio o no la contraseña desde la creación de su cuenta.

* **Formula:** =SI(**G2**=FECHA(1970;1;1);"No cambió";"Cambió")
* La configuración del formato de la celda es “General”.
1. Ejecutar los siguientes controles sobre los archivos:

**Listado de usuarios habilitados:**

* Verificar que el DisplayName que aparece en la columna UserName, coincida con el nombre y apellido de los usuarios al cual está asignado. En referencia a los usuarios administradores, deben estar creados con la nomenclatura apropiada en caso de estar formalizada en la política de Seg. de la información o el usuario administrador este referenciado al usuario asignado.
* Verificar la columna Account Flags para validar el estado del usuario. Ver tabla adjunta.

| **Bandera** | **Descripción** |
| --- | --- |
| D | Cuenta deshabilitada. |
| H | Se requiere un directorio de inicio. |
| I | Una cuenta de confianza entre dominios. Se requiere un directorio de inicio. |
| L | La cuenta ha sido bloqueada automáticamente. |
| M | Una cuenta de inicio de sesión de MNS (servicio de red de Microsoft). |
| N | No se require contraseña. |
| S | Cuenta de confianza de servidor. |
| T | Entrada temporal de una cuenta duplicada. |
| U | Cuenta normal de usuario. |
| W | Estación de trabajo de confianza. |
| X | La contraseña no expira |

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 cuantos usuarios están deshabilitado. Esto se logra al filtrar una columna.
* Columna Account Flags contendiendo las banderas “[UD ]” entre otras.

**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 cuantos usuarios no les expira la contraseña. Esto se logra al filtrar una columna.
* Columna Account Flags contendiendo las banderas “[UX ]” entre otras.
* 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 están sin contraseña**

* Verificar cuantos usuarios están sin contraseña. Esto se logra al filtrar una columna.
* Columna Nunca Cambió Contraseña con el parámetro “No Cambio”.
* Aquellos usuarios que están activos se deben verificar que no tengan habilitada la opción de requiere 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 cambian contraseña**

* Verificar la columna “Nunca Cambió Contraseña” para validar los usuarios que no cambian contraseña. Esto se logra filtrando varias columnas:
* Columna Nunca Cambió Contraseña con el parámetro “Cambió”.
* Columna Infringe Política con el parámetro “Sí”.
* Columna Account Flags con la bandera “[U ]”, sin la bandera “X” que indica que les expira la contraseña, y sin la bandera “D” que indica que las cuentas están desactivadas.
* Aquellos usuarios que están activos se deben verificar que no tengan habilitada la opción de requiere contraseña, de ser así se debe modificar este parámetro y marcar la opción cambiar contraseña en el siguiente inicio de sesión.

# Nota General

Se debe tener en cuenta que pueden existir una variedad de combinaciones en las banderas, lo importante es validar que los valores asignados en la bandera estén presentes en el control que estamos realizando.

Ejemplo: Este ejemplo mostrara dos usuarios que tienen banderas similares.

| **Bandera** | **Descripción** |
| --- | --- |
| D | Cuenta deshabilitada. |
| N | No se require contraseña. |
| U | Cuenta normal de usuario. |
| X | La contraseña no expira |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UserName** | **Account Flags** | **Total U** | **Total D** | **Total N** | **Total X** |
| User1 | “[UDX ]” | 1 | 1 |   | 1 |
| User2 | “[UDN ]” | 1 | 1 | 1 |   |

El informe final detallará entonces:

* Cuentas normal de usuario = 2
* Cuentas deshabilitadas = 2
* Cuenta que no requiere contraseña = 1
* Cuenta en que contraseña no expira = 1

# 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** |
|  |  |  |

