**PROGRAMA DE TRABAJO**

**AUDITORÍA**

**CONTROLADOR DE DOMINIO**

**WINDOWS ACTIVE DIRECTORY**

Curso Práctico Auditoría de Sistemas

**Introducción**

El Controlador de Dominio es un servidor central utilizado para la administración de un dominio de red, este tiene una serie de responsabilidades como la de autenticación, que es el proceso de permitir o denegar a un usuario el acceso a equipos de cómputo y recursos compartidos en una red a través del uso de cuentas de usuarios y contraseñas. Esto permite validar a los usuarios para ser partes de la plataforma de clientes que recibirán los servicios de información.

El Active Directory (AD) o Directorio Activo, de forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos como usuarios y grupos, con el objetivo de administrar el acceso a los equipos y recursos conectados a la red. Windows Active Directory proporciona un sistema de inicio de sesión integrado que aborda la seguridad, el acceso y la administración de identidades.

El entorno típico de Windows está compuesto por servidores dedicados a tareas específicas. Cada dispositivo en un dominio confía en el servidor de Active Directory y le permite autenticar y aprobar la acción que cada usuario está intentando realizar, ya sea en la red o en el equipo local.

Active Directory proporciona un repositorio central que contiene ID de usuario, permisos y procesamiento de auditoría.

**Riesgos relacionados**

Si no se diseñan y administran controles efectivos de Active Directory, se pueden producir: Interrupción de los servicios informáticos, Destrucción de datos empresariales, Divulgación de información sensible, violacion de propiedad intelectual, perdida reputacional y de confianza, Multas, sanciones, Pérdida de productividad y Brechas de seguridad.

**Objetivo del Programa**

Validar que los parámetros de configuración relacionados a la seguridad del Controlador de Dominio Active Directory están establecidos de acuerdo a las mejores prácticas de seguridad. Estas son mejores prácticas sugeridas por el fabricante Microsoft y por estándares globales de ciberseguridad.

**Alcance:**

Servidor Controlador de Dominio Windows Active Directory.

**Auditor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Fecha: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PASOS DEL PROGRAMA DE AUDITORIA.**

**1. Logs y Directorios Críticos**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1.1 Determinar si la auditoría de accesos al Directory Service está habilitada, llevando a cabo los siguientes pasos:**

1. *Abra el group policy editor centrado en los controladores de dominio OU (por defecto: default: Domain Controller Security Policy).*
2. *Vaya a la siguiente ubicación sub-árbol: Windows Settings\Security Settings\Local Policies\Audit Policy.*
3. *Haga doble clic en la opción de auditoría “Audit Directory Service Access”.*
4. *Determinar si la casilla “define these policy settings” está seleccionada y que las casillas de éxito y fracaso están seleccionadas.*

**Fecha:**

30 de septiembre 2020

**Trabajo realizado:**

Con asistencia de José Pérez, Administrador de Servidores, de manera presencial observamos los parámetros de auditoria del servidor Controlador de Dominio “DC-SERVER” donde identificamos que el parámetro “Audit Directory Service Access” está activo y configurado para registrar los intentos de accesos fallidos lo cual es apropiado de acuerdo con las mejores prácticas de seguridad.

Ver evidencias de esta revisión en el archivo “Evidencia-1”

**Conclusión:**

El parámetro “Audit Directory Service Access” está configurado de acuerdo a las mejores prácticas de seguridad.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1.2 Determinar si la auditoría de eventos de inicio de sesión de cuentas (Audit Account Logon Events) está habilitada para intentos fallidos, mediante la realización de los siguientes pasos:**

1. *Abra el Group Policy Editor centrado en el objeto apropiado.*
2. *Vaya a la siguiente ubicación: Computer Configuration\WindowsSettings\Security Settings\Local Policies\Audit Policy.*
3. *Doble click en la opción 'Audit Account Logon Events'".*
4. *Determinar si la casilla de verificación “failure” está seleccionada.*

**Fecha:**

**Trabajo realizado:**

**Conclusión:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1.3 Determinar si sólo el personal apropiado tiene acceso a archivos críticos del Sistema Operativo mediante la realización de los siguientes pasos:**

1. *Haga click derecho en el archivo en el Explorador de Windows.*
2. *Seleccione Propiedades en el menú.*
3. *Seleccione la ficha Seguridad.*
4. *Haga clic en el botón Opciones avanzadas.*
5. *Comparar los permisos actuales con las recomendaciones.*
6. *Repita el procedimiento para todos los archivos de la lista.*

*Archivos:*

*%systemroot%\system32\config\SOFTWARE*

*%systemroot%\system32\config\SECURITY*

*%systemroot%\system32\config\SYSTEM*

*Las directrices recomendadas establecen que el privilegio “Full Control” sólo lo deben tener las cuentas:*

* *Administrators*
* *System*

**1.4 Determinar si los permisos en los directorios críticos indicados más abajo cumplen con las recomendaciones de mejores prácticas mediante la realización de los siguientes pasos:**

1. *Haga click derecho en el directorio en el Explorador de Windows.*
2. *Seleccione Properties.*
3. *Seleccione la pestaña Security.*
4. *Compare los permisos actuales con los recomendados.*

Directorios:

%systemroot%\sysvol

%systemroot%\security

%systemroot%\ntfrs

%systemroot%\ntds

Las guías recomendadas establecen:

- Administrators - Full Control

- System - Full Control

- Creator Owner - Full Control

- TrustedInstaller - Full Control

**2. Directorios compartidos y relaciones de confianza**

**2.1 Revisar la lista de directorios compartidos ejecutando el siguiente comando desde la ventana del cmd:**

* *Net Share*

Si existen directorios compartidos que no sean los predeterminados del controlador de dominio (por ejemplo, C$, IPC$, SYSVOL, Netlogon), utilizar el Explorador de Windows para ver los permisos sobre estos directorios. Pregunte al administrador del sistema, por qué se requieren estos directorios.

**2.2 Determinar que las relaciones de confianza entre el Controlador de Dominio y otros servidores son restringidas y que sólo se permiten si es estrictamente necesario:**

1. *Haga click en Start - Programs - Administrative Tools - Active Directory Domains and Trusts.*
2. *Haga click derecho sobre el nombre del dominio.*
3. *Seleccione Propiedades.*
4. *Seleccione la pestaña Trusts.*
5. *Verificar lo adecuado de las relaciones de confianza que aparecen en la pestaña Trusts.*

**3. Servicios de Red.**

**3.1 Determine si el servicio telnet se ha desactivado mediante la realización de los siguientes pasos:**

1. *Abra el regedit.*
2. *Asegúrese de que no existen las siguientes llaves de registro:*
3. *HKLM\SYSTEM\CurrentControlSet\Services\TlntSvr HKLM\SOFTWARE\Microsoft\TelnetServer*
4. Cierre regedit.

**3.2 Determinar si el servicio SNMP está activo mediante la revisión de los servicios en el snap-in Services. Si el SNMP está activo examine que posea community strings validos realizando lo siguiente:**

1. *Abra el editor de Group Policy centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Haga doble click en la pestaña Computer Configuration.*
3. *Haga doble click en la pestaña Administrative Templates.*
4. *Haga doble click en la pestaña Network.*
5. *Haga doble click en la pestaña SNMP.*
6. *Haga doble click en el sub-opción apropiada (es decir, community).*
7. *Determinar si el botón de activo está seleccionado.*

**4. Parámetros de contraseñas**

**4.1 Verifique con el administrador del sistema, que la casilla User Must Change Password at Next Logon se encuentra seleccionada al momento de crear nuevas cuentas.**

**4.2 Determinar si el historial de contraseñas está siendo aplicado, mediante la realización de los siguientes pasos:**

1. *Abra el group policy editor centrado en el dominio OU (por defecto: Domain Security Policy).*
2. *Vaya a la siguiente ubicación: Windows Settings\Security Settings\Account Policies\Password Policies.*
3. *Haga doble click en la política: Enforce Password History*
4. *Revise el valor del Password History. Esta debe estar establecido de acuerdo con los estándares corporativos y mejores prácticas.*

**4.3 Determinar si la edad mínima de la contraseña está siendo aplicada apropiadamente, mediante la realización de los siguientes pasos:**

1. *Abra el group policy editor centrado en el dominio OU (por defecto: Domain Security Policy).*
2. *Vaya a la siguiente ubicación: Windows Settings\Security Settings\Account Policies\Password Policies.*
3. *Haga doble clic en la política Minimum password age.*
4. *Revise el valor del Minimum password age. Este se debe establecer de acuerdo con los estándares corporativos y las mejores prácticas.*

**4.4 Determinar si la edad máxima de la contraseña está siendo aplicada apropiadamente mediante la realización de los siguientes pasos:**

1. *Abra el group policy editor centrado en el dominio OU (por defecto: Domain Security Policy).*
2. *Vaya a la siguiente ubicación: Windows Settings\Security Settings\Account Policies\Password Policies.*
3. *Haga doble clic en la política Maximum password age.*
4. *Revise el valor del Maximum password age. Esto se debe establecer de acuerdo con los estándares corporativos y las mejores prácticas.*

**4.5 Determinar si la longitud mínima de la contraseña es adecuada mediante la realización de los siguientes pasos:**

1. *Abra el group policy editor centrado en el dominio OU (por defecto: Domain Security Policy).*
2. *Vaya a la siguiente ubicación: Windows Settings\Security Settings\Account Policies\Password Policies.*
3. *Haga doble clic en la política Minimum password length.*
4. *Revise el valor del Minimum password length. Esto se debe establecer de acuerdo con los estándares corporativos.*

**4.6 Determinar si el parámetro “Password must meet complexity requirements” está habilitado mediante la realización de los siguientes pasos:**

1. *Abra el group policy editor centrado en el dominio OU (por defecto: Domain Security Policy).*
2. *Vaya a la siguiente ubicación: Windows Settings\Security Settings\Account Policies\Password Policies.*
3. *Haga doble clic en la política Password must meet complexity requirements.*
4. *Revise el valor. Esto se debe establecer de acuerdo con los estándares corporativos y mejores prácticas.*

**4.7 Determinar si el parámetro “Store passwords using reversible encryption” está inhabilitado mediante la realización de los siguientes pasos:**

1. *Abra el group policy editor centrado en el dominio OU (por defecto: Domain Security Policy).*
2. *Vaya a la siguiente ubicación: Windows Settings\Security Settings\Account Policies\Password Policies.*
3. *Haga doble clic en la política “Store passwords using reversible encryption”.*
4. *Revise el valor. Esto se debe establecer de acuerdo con los estándares corporativos y mejores prácticas.*

**4.8 Determinar con el Administrador del Controlador de Dominio, que las contraseñas de las cuentas de nivel de administrador se están cambiando de acuerdo con las normas de seguridad de la empresa.**

1. *Comando: net user administrator*

**4.9 Para una selección de usuarios, determinar si el privilegio de evadir las políticas de sobre cambio de contraseñas se ha desactivado mediante la realización de los siguientes pasos:**

1. *Abra el Active Directory Users and Computers.*
2. *En el árbol de consola, haga doble click en el nodo de dominio apropiado y, a continuación, seleccione el contenedor Usuarios.*
3. *Haga doble click en cada cuenta.*
4. *Determinar si las opciones User Cannot Change Password and the Password Never Expires no están marcadas.*
5. *Haga click en cancelar para cerrar el cuadro de diálogo.*
6. *Repita el procedimiento para cada cuenta de usuario.*

**4.10 Verificar que las características de bloqueo de cuentas (account lockout) estén habilitadas y los parámetros configurados acorde con las mejores prácticas.**

1. *Abra el group policy editor centrado en el sistema local (es decir, local security policy).*
2. *Vaya a la siguiente ubicación subárbol: Security Settings\Account Policies\Account Lockout*
3. *Haga doble click en la política: Account Lockout Duration.*
4. *Asegúrese de que la opción está activada y con un valor adecuado.*
5. *Haga click en Cancelar.*
6. *Haga doble click en la política: Account Lockout Threshold.*
7. *Asegúrese de que la opción está activada y con un valor adecuado.*
8. *Haga click en Cancelar.*
9. *Haga doble click en la política: "Reset account lockout counter after"*
10. *Asegúrese de que la opción está activada y con un valor adecuado.*
11. *Haga click en Cancelar.*

**5. Grupos de altos privilegios**

**5.1 Determine si sólo usuarios autorizados son miembros de los grupos privilegiados: Backup Operators, Server Operators, Account Operators, y Print Operators en el servidor de dominio mediante la realización de los siguientes pasos:**

1. *Abra el Active Directory Users and Computers.*
2. *Seleccione el contenedor predeterminado.*
3. *Haga doble click en el grupo local Backup Operators.*
4. *Seleccione la pestaña de miembros.*
5. *Determinar si solamente posee cuentas de usuarios autorizadas.*
6. *Haga click en el botón Cancelar.*
7. *Repita los pasos c-e para los Server Operators, Print Operators y Account Operators.*

**5.2 Después de conversar con el administrador del dominio o el encargado de la gestión de accesos sobre usuarios y roles de usuario, lleve a cabo los siguientes pasos:**

1. *Abra el Active Directory Users and Computers.*
2. *Expanda el contenedor incorporado.*
3. *Haga doble click en el grupo Administradores.*
4. *Seleccione la pestaña “miembros” y verifique los miembros de este grupo.*
5. *Haga click en Cancelar.*
6. *Expanda el contenedor de usuarios.*
7. *Haga doble click en el grupo Domain Admins group.*
8. *Seleccione la pestaña “miembros” y revise la membresía de este grupo.*
9. *Haga click en Cancelar.*
10. *Haga doble click en el grupo Enterprise Admins.*
11. *Seleccione la pestaña “miembros” y la revisión de miembro de este grupo.*
12. *Haga clic en Cancelar.*
13. *Cierre Active Directory Users and Computers.*

**6. Configuraciones de cuentas de usuarios**

**6.1 Verifique que las cuentas Administrator, Guest y *Support\_388945a0* han sido protegidas mediante la realización de los siguientes pasos:**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Navege por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.*
3. *Asegúrese: Que el estado de la cuenta Administrador esté configurado en Activado.*
4. *Asegúrese: Que el estado de la cuenta de Guest está configurado en desactivado.*
5. *Asegúrese: Que la cuenta renombrada administrator esté establecida de acuerdo a las mejores prácticas.*
6. *Asegúrese: Que la cuenta renombrada Guest esté desactivada.*
7. *Abra el Local Users and Groups MMC Snap-in.*
8. *Seleccione la carpeta usuarios.*
9. *Asegúrese de que la cuenta Support\_388945a0 esté deshabilitada o eliminada.*

**6.2 Verificar en la sección Security Options del Group Policy editor que el parámetro “Accounts: Guest account status” se encuentre desactivado.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Navege por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.*
3. *Parámetro “Accounts: Guest account status”.*

**6.3 Verificar en la sección “Security Options” del Group Policy editor que el parámetro “Accounts: Limit local account use of blank passwords to console logon only” se encuentre Activo.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Navege por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.*

**6.4 Verificar que la cuenta de administración local “Administrator” de las estaciones de trabajo se encuentran renombradas a través del Group Policy editor, parámetro “Accounts: Rename administrator account”**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Navege por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.*

**6.5** **Verificar en la sección “Security Options” del Group Policy editor que el parámetro “Recovery console: Allow automatic administrative logon” se encuentre desactivado.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Navege por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.*

**7. Parámetros de accesos**

7.1 **Verificar el privilegio de usuario Access this Computer from the Network, sólo los grupos autorizados deben tener este privilegio.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro de Active Directory.*
2. *Vaya a la siguiente ubicación: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Haga doble click en el privilegio Access this Computer from the Network.*

Las directrices recomendadas establecen:

- Administrators, (incluyendo Domain admins).

- Cualquiera de los grupos locales o de dominio que contienen los usuarios que deben tener acceso a recursos en este servidor.

7.2 **Compruebe que los grupos apropiados han sido asignados a la opción "Allow log on locally" realizando los siguientes pasos:**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio de Allow log on locally está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

Las directrices recomendadas son las siguientes:

- Administradores, Administradores de dominio

**7.3** **Compruebe que los grupos apropiados han sido asignados a la opción "Act as part of the operating system"**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “Act as part of the operating system” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.4 Compruebe que los grupos apropiados han sido asignados a la opción "Add workstations to domain":**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.5 Compruebe que la cuenta local Guest está incluida en la configuración del parámetro “Deny access to this computer from the network”**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.6 Compruebe que la cuenta local Guest está incluida en la configuración del parámetro “Deny log on locally”.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “Deny log on locally” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.7 Compruebe que el privilegio “Generate security audits” sólo lo posee asignado las cuentas Local Service y Network Service.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “Generate security audits” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.8 Compruebe que el privilegio “Load and unload device drivers” sólo lo posee asignado las cuentas Administrators y Print Operators.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “Load and unload device drivers” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.9 Compruebe que el privilegio “Manage auditing and security log” sólo lo posee asignado el grupo de usuarios Administrators.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “Manage auditing and security log” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**7.10 Compruebe que el privilegio “Shut down the system” sólo lo posee asignado el grupo de usuarios Administrators.**

1. *Abra el Group Policy editor centrado en el equipo local o unidad organizativa apropiada dentro del Active Directory.*
2. *Desplácese por la siguiente ruta: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.*
3. *Asegúrese de que el privilegio “Shut down the system” está definido y que los grupos apropiados han sido asignados en conformidad con las normas corporativas o las directrices recomendadas.*

**8 Parches y actualizaciones**

**8.1 Determinar, mediante la búsqueda en la página principal de Microsoft (http://www.microsoft.com/), la última versión del sistema disponibles. Asegúrese de que los parches apropiados están instalados en el servidor.**