	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	1 / 21

LABORATORIO N°8: Seguridad en Servidores Windows usando GPOs




ÍNDICE

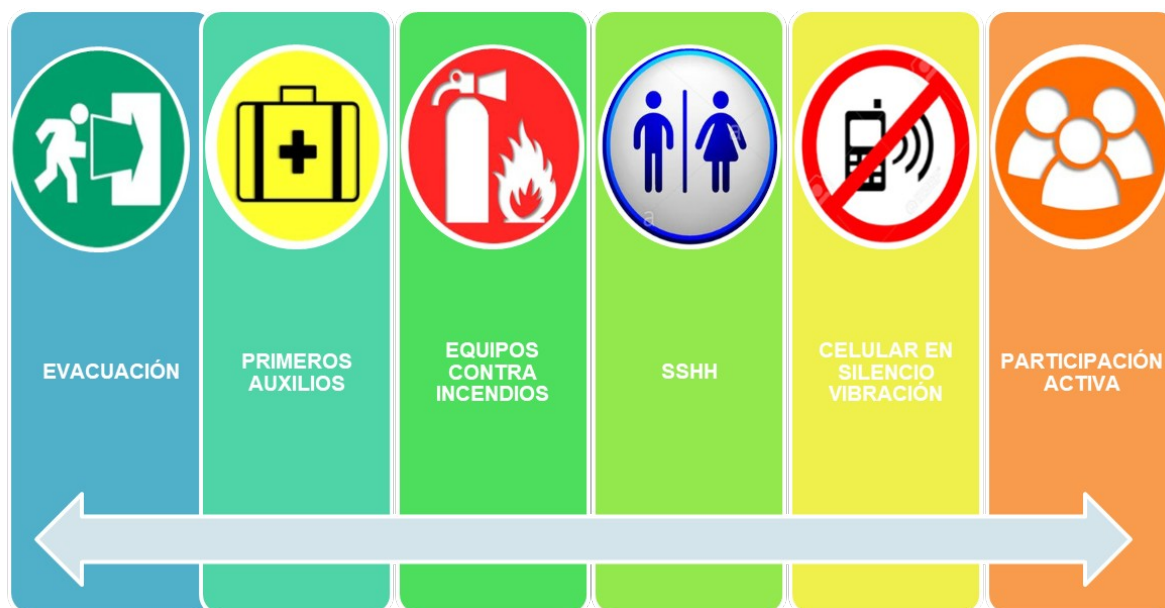
RECOMENDACIONES GENERALES DE SEGURIDAD.....	2
1. OBJETIVOS.....	4
2. DOCUMENTOS O NORMAS DE REFERENCIA.....	4
3. DESCRIPCIÓN DEL PROCESO.....	4
3.1 FUNDAMENTO TEÓRICO.....	4
3.2 RECURSOS.....	6
3.3 DESCRIPCIÓN DEL PROCESO.....	7
4. EVALUACIÓN.....	11
5. OBSERVACIONES Y CONCLUSIONES.....	12
6. ANEXOS.....	12

Historial de revisión				
Participantes		Área	Fecha	Firma
Elaborado por	Adriana Arista Valdivia	Tecnología Digital y Gestión		
Revisado por	Alfredo Saire Huamán	TDyG		
Aprobado por	Alfredo Saire Huamán	TDyG		

Control de cambios		
Revisión	Fecha	Descripción del Cambio

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	2 / 21

RECOMENDACIONES GENERALES DE SEGURIDAD




1. Condiciones obligatorias para el uso del ambiente

- Prohibida la manipulación de hardware, conexiones eléctricas o de red.
- Ubicar maletines y/o mochilas de manera ordenada en el aula de Laboratorio o en los casilleros asignados al estudiante.
- No ingresar con líquidos, ni comida al aula de Laboratorio.
- Al culminar la sesión de laboratorio apagar correctamente la computadora y la pantalla, y ordenar las sillas utilizadas.

2. Respuesta a emergencias

- Vías de acceso y evacuación
Puerta de Salida del laboratorio hacia el costado derecho siguiendo por el lado derecho en dirección a hacia las escaleras de emergencia. El punto de reunión en la parte posterior del edificio.
- Equipos de respuesta a emergencias
Extintor de CO2
- Señalización de seguridad
Zona segura en caso de sismos, Salida.

3. Normas de seguridad generales

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	3 / 21

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	5 / 21

1. OBJETIVOS

- Utilizar GPO para asegurar servidores miembros del dominio.
- Auditar los inicios de sesión al dominio.
- Configurar el firewall de Windows.

2. DOCUMENTOS O NORMAS DE REFERENCIA

- Revisar material teórico compartido en Canvas como: Diapositivas, Texto oficial del curso y enlaces de interés.

3. DESCRIPCIÓN DEL PROCESO

3.1 FUNDAMENTO TEÓRICO

Escenario

Ha estado trabajando para ACME como especialista en soporte de escritorio y ha visitado computadoras de escritorio para solucionar problemas de red y aplicación. Recientemente ha aceptado una promoción para el equipo de soporte de servidor. Una de sus primeras tareas es configurar el servicio de infraestructura para una nueva sucursal.

Su administrador la ha dado algunos parámetros de seguridad que necesitan ser implementados en todos los servidores miembros del dominio. También, necesita implementar la auditoría para una carpeta compartida utilizada por el departamento de Marketing. Finalmente, necesita implementar la auditoría para el inicio de sesión al dominio.

3.2 RECURSOS

3.2.1 Charla de seguridad 5 minutos

Toda sesión de aprendizaje debe iniciar con una charla de seguridad de 5 minutos, donde el docente explique claramente las normas de seguridad básicas a cumplir durante la sesión.

3.2.2 Implementos de Seguridad de uso obligatorio (NO APLICA)

3.2.3 Materiales e insumos (NO APLICA)

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	6 / 21

3.2.4 Equipos

Una computadora con:

- Windows 7 o superior
- VMware Workstation 10+ o VMware Player 7+
- Conexión a la red del laboratorio

Máquinas virtuales:

- LON- DC1
- LON-SVR-A
- LON-CL1

DVD o ISO:

- Windows Server 2012
- Windows Server 2016
- Windows 10

3.2.5 Herramientas (NO APLICA)

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	7 / 21


3.3 DESCRIPCIÓN DEL PROCESO

Lab Setup

1. Encender la máquina virtual LON-DC1 e iniciar sesión como Administrador del dominio.
2. Encender la máquina virtual LON-SVR-A (Lab06), verificar que es un servidor Miembro del dominio y no un Controlador del Dominio.
3. Encender la máquina virtual LON-CL1, verificar que es miembro del dominio.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	8 / 21

EJERCICIO 1: Uso del GPO para asegurar los servidores miembros del dominio

ETAPA DEL PROCESO	PELIGROS POTENCIALES	RIESGO	CONTROLES
Ejercicio 01: Uso del GPO para asegurar los servidores miembros del dominio	Electricidad	Riesgo eléctrico 	Uso de supresores de pico

Escenario

ACME usa el grupo Administradores de Computadoras para proveer administradores con permisos para administrar servidores miembros. Como parte del proceso de instalación para un nuevo servidor, el grupo Administradores de Computadoras del dominio es agregado al grupo local Administradores en el nuevo servidor. Recientemente, este paso importante se ha olvidado cuando se han configurado los nuevos servidores.


Para asegurar que el grupo Administradores de Computadoras siempre tenga permisos para administrar los servidores miembros, el administrador le ha pedido crear un GPO que defina la membresía del grupo local Administradores en los servidores miembros para incluir el grupo Administradores de Computadoras. Este GPO también habilitará el modo de aprobación de administrador para el UAC (User Account Control)

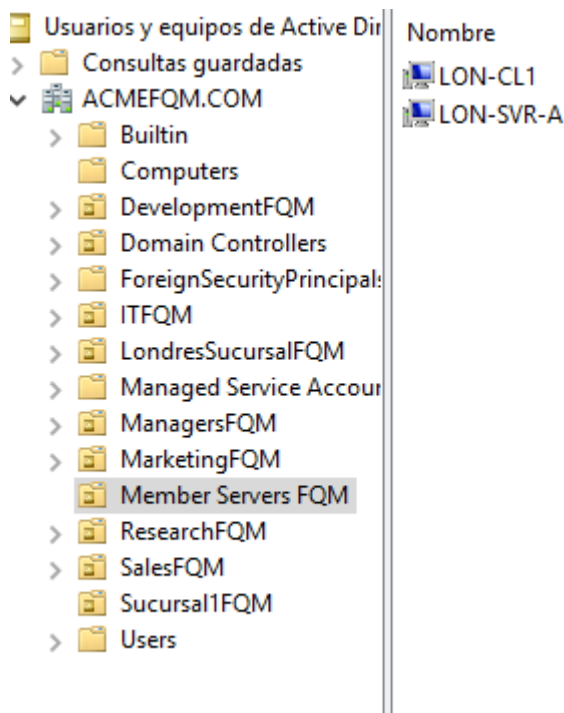
Las principales tareas para este ejercicio son las siguientes:

- Crear un OU para los servidores miembros.
- Crear un grupo Administradores de servidores.
- Crear un GPO para asegurar los servidores miembros.
- Configurar la membresía del grupo local Administradores.
- Modificar el GPO creado según los requerimientos solicitados.

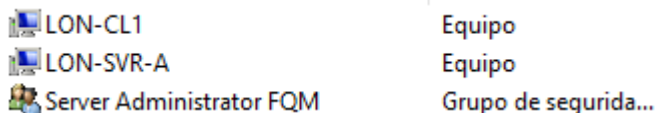
*** Reemplazar XYZ por las iniciales de su primer nombre, apellido paterno y apellido materno.

1. Crear un OU para los servidores miembro.
 - En LON-DC1 abrir la herramienta **Usuarios y equipos de Active Directory**.
 - Crear un nuevo OU con el nombre de **Member Servers XYZ**.
 - Mover los objetos **LON-SVR-A** y **LON-CL1** del OU Computers al OU **Member Servers XYZ**.

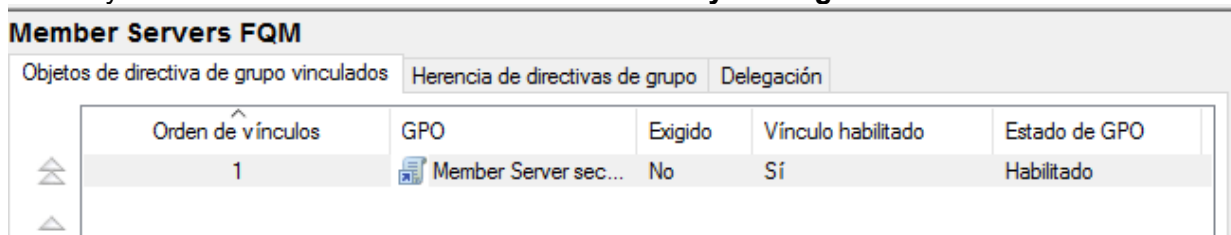
	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	9 / 21



2. Crear un grupo para los administradores de los servidores.
 - En el OU **Member Servers XYZ** crear un nuevo grupo global de seguridad con el nombre **Server Administrators XYZ**.



3. Crear un GPO para el OU Member Servers.
 - En LON-DC1 abrir la herramienta **Administración de directivas de grupo**.
 - En el contenedor **Objetos de directiva de grupo** crear un nuevo GPO con el nombre **Member Server Security Settings XYZ**.
 - En el OU **Member Servers**, hacer clic derecho y seleccionar **Vincular GPO existente** y vincularla a la GPO **Member Server Security Settings XYZ**.



4. Configurar el GPO creado para definir la membresía de los grupos de administración.
 - En LON-DC1 abrir la herramienta **Administración de directivas de grupo**.
 - Editar el GPO **Default Domain Policy**.
 - Expandir **Configuración del equipo** -> **Directivas** -> **Configuración de Windows** -> **Configuración de seguridad** -> **Grupos restringidos**.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	10 / 21

- En el panel derecho, hacer clic derecho y seleccionar **Agregar Grupo...** luego clic en **Examinar...** y procedemos a agregar el grupo **Server Administrators** al grupo **Administradores**.
- También agregar el grupo **Admins. del dominio** al grupo **Administradores**.

Nombre de grupo	Miembros	Miembro de
 ACMEFQM\Admins. del dominio		Administrador...
 ACMEFQM\Server Administrator FQM		Administradores

5. Verificar que el GPO funciona correctamente.

- En LON-CL1 abrir una ventana de comandos y ejecutar el siguiente comando para aplicar las directivas GPO:
 - **gpupdate /force**

```

Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>gpupdate/force
"gpupdate" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.


C:\Users\Administrador>gpupdate /force
Actualizando directiva...

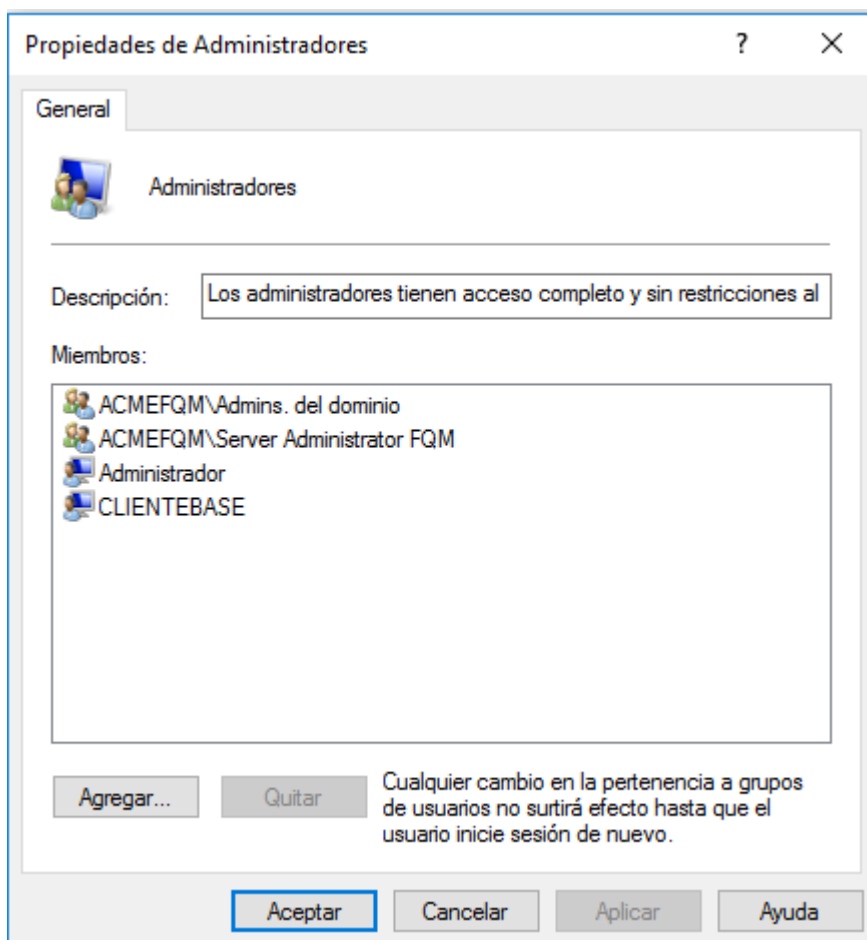
La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

C:\Users\Administrador>_

```

- Ejecutar el programa **Administración de equipos**, en **Usuarios y grupos locales** ubicar el grupo **Administradores** y ver los objetos que son miembros de dicho grupo.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	11 / 21



- ¿Qué objetos grupo de usuario son miembros del grupo Administradores?

Admins. Del dominio y server administratorsFQM lo que prueba que la directiva se aplico correctamente

Entregable 1. Capture la pantalla donde se muestre el resultado de los pasos 4 y 5.

6. Modificar la configuración del GPO **Member Server Security Settings XYZ** para evitar que los usuarios inicien sesión localmente en los servidores.
 - En LON-DC1 editar el GPO **Member Server Security Settings XYZ**.
 - Expandir **Configuración del equipo** -> **Directivas** -> **Configuración de Windows** -> **Configuración de seguridad** -> **Directivas locales** -> **Asignación de derechos de usuario**.
 - Hacer doble clic en la directiva **Permitir el inicio de sesión local** y configurarla para conceder este permiso a los grupos **Administradores** y **Admins. del dominio**.
 - Cerrar el editor de directivas.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	12 / 21

☒ Definir esta configuración de directiva:

ACMEFQM\Admins. del dominio
Administradores


Agregar usuario o grupo...

Quitar

7. Modificar la configuración del GPO **Member Server Security Settings XYZ** para habilitar el control de cuentas de usuario en el modo administrador.
 - En LON-DC1 editar el GPO **Member Server Security Settings XYZ**.
 - Expandir **Configuración del equipo -> Directivas -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad**.
 - Habilitar la directiva **Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador**.
 - Cerrar el editor de directivas.

Propiedades: Control de cuentas de usuario: Modo de apr... ? X

Configuración de directiva de seguridad Explicación

 Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador


☒ Definir esta configuración de directiva:

☒ Habilitada

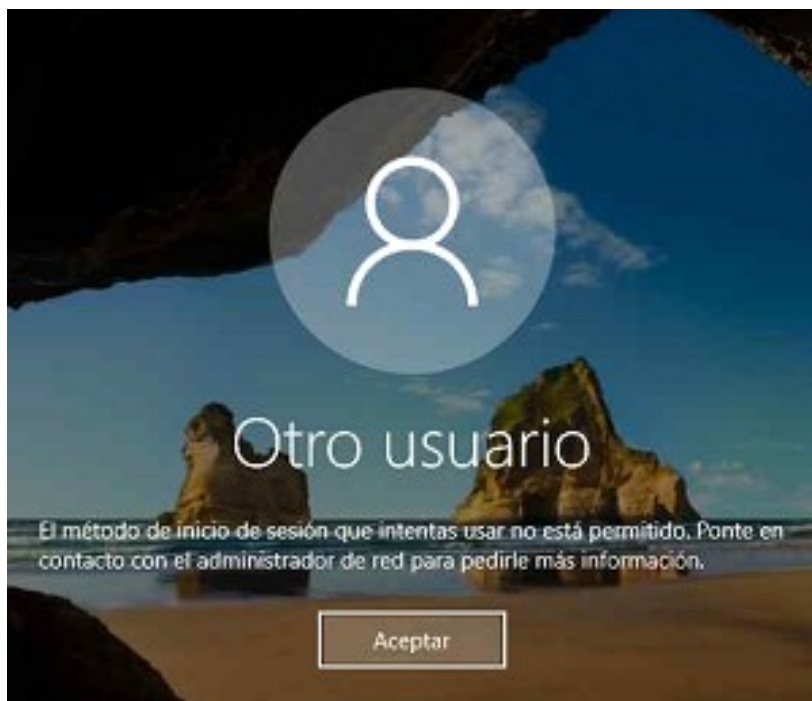
☐ Deshabilitada

Aceptar Cancelar Aplicar


8. Verificar que un usuario que no pertenece al grupo Administradores no inicia sesión en LON-SVR-A o LON-CL1.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	13 / 21


Importante: Recuerde reiniciar el servidor para que las directivas (GPO) se apliquen.



Entregable 2. Capture la pantalla donde se muestre el resultado del paso 13.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	14 / 21

EJERCICIO 2: Auditando el inicio de sesión

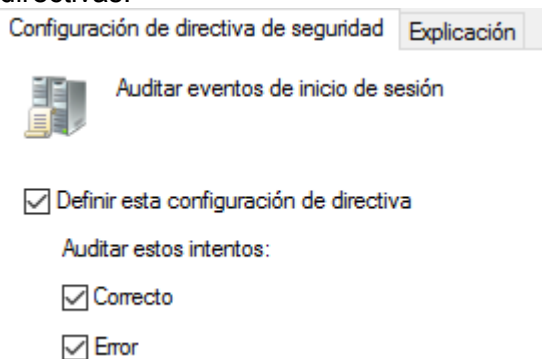
ETAPA DEL PROCESO	PELIGROS POTENCIALES	RIESGO	CONTROLES
Ejercicio 2: Auditando el inicio de sesión	Electricidad	Riesgo eléctrico 	Uso de supresores de pico

Escenario

Después de una revisión de la seguridad, el comité de directivas de TI ha decidido realizar el seguimiento al inicio de sesión de todos los usuarios del dominio. Su administrador le ha pedido habilitar la auditoría del inicio de sesión y verificar su funcionamiento.


Las principales tareas para este ejercicio son las siguientes:

- Modificar el GPO Default Domain Policy.
 - Verificar el funcionamiento del GPO.
9. Modificar el GPO Default Domain Policy.
- En LON-DC1 editar el GPO **Default Domain Policy**.
 - Expandir **Configuración del equipo** -> **Directivas** -> **Configuración de Windows** -> **Configuración de seguridad** -> **Directivas locales** -> **Directiva de auditoría**.
 - Habilitar la directiva **Auditar eventos de inicio de sesión** con ambos intentos: **Correcto** y **Error**.
 - Cerrar el editor de directivas.



10. Refresque las directivas aplicadas al miembro del dominio.

- En LON-CL1 como Administrador ejecutar **gpupdate /force**.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	15 / 21


```
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

C:\Users\Administrador>_
```

11. En LON-CL1 intente iniciar sesión con la cuenta de usuario **Adam** pero con la contraseña errónea. (Intente 6 veces aproximadamente.)
12. En LON-CL1 intente iniciar sesión con una cuenta de usuario inexistente.
13. En LON-CL1 iniciar sesión con una cuenta de usuario **Adam** y la contraseña correcta.
14. Revisar los eventos de los inicios de sesión erróneos.
 - En LON-DC1 ejecutar la herramienta **Visor de eventos**.
 - Expandir **Registro de Windows** -> **Seguridad**.
 - Verificar que los eventos con ID **4624, 4634, 4771, 4672 o similares** se muestren en la ventana.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	16 / 21

Seguridad Número de eventos: 29.825 (!) Nuevos eventos disponibles

Palabra...	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Audi...	09/06/2020 6:29:01	Microsoft Win...	4634	Cerrar sesión
Audi...	09/06/2020 6:29:01	Microsoft Win...	4627	Pertenencia a grupos
Audi...	09/06/2020 6:29:01	Microsoft Win...	4624	Inicio de sesión
Audi...	09/06/2020 6:29:01	Microsoft Win...	4672	Inicio de sesión especial
Audi...	09/06/2020 6:28:56	Microsoft Win...	4634	Cerrar sesión
Audi...	09/06/2020 6:28:02	Microsoft Win...	4634	Cerrar sesión
Audi...	09/06/2020 6:28:02	Microsoft Win...	4627	Pertenencia a grupos
Audi...	09/06/2020 6:28:02	Microsoft Win...	4624	Inicio de sesión
Audi...	09/06/2020 6:28:02	Microsoft Win...	4672	Inicio de sesión especial
Audi...	09/06/2020 6:27:59	Microsoft Win...	4634	Cerrar sesión
Audi...	09/06/2020 6:27:37	Microsoft Win...	4634	Cerrar sesión

Evento 4634, Microsoft Windows security auditing.

General Detalles

Nivel: Información Palabras clave: Auditoría correcta


Usuario: No disponible Equipo: LON-DC1.ACMEFQM.COM

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Entregable 3. Capture la pantalla donde se muestre el resultado del paso 14.

EJERCICIO 3: Configurando Políticas de Firewall de Windows

ETAPA DEL PROCESO	PELIGROS POTENCIALES	RIESGO	CONTROLES
Ejercicio 3: Configurando Políticas de Firewall de Windows	Electricidad	Riesgo eléctrico 	Uso de supresores de pico

Escenario

Su administrador le ha pedido configurar las reglas de Firewall de Windows para un conjunto de nuevas aplicaciones en los servidores. Estas aplicaciones tienen una aplicación web que utiliza un puerto no estándar. Usted necesita configurar el Firewall de Windows para permitir la comunicación a través de este puerto. Usted utilizará el filtrado de seguridad para asegurarse que las nuevas reglas se apliquen solo a las nuevas aplicaciones de los servidores.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	17 / 21

Las principales tareas para este ejercicio son las siguientes:

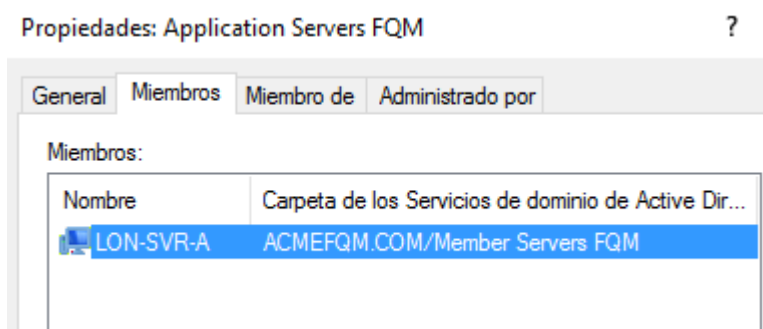
- Crear un grupo para los servidores que ejecutarán las aplicaciones.
- Crear un GPO para estos servidores.
- Configurar el GPO para configurar las reglas del Firewall de Windows.
- Verificar el funcionamiento.

15. Crear un grupo para los servidores de aplicaciones.

- En LON-DC1 crear el grupo global de seguridad **Application Servers XYZ** en el OU **Member Servers XYZ**.

Nombre	Tipo	Descripción
LON-CL1	Equipo	
LON-SVR-A	Equipo	
Server Administrator FQM	Grupo de seguridad...	
Application Servers FQM	Grupo de seguridad...	

- Agregar el servidor **LON-SVR-A** al grupo **Application Servers XYZ**.




16. Crear el GPO con el nombre **Application Servers Firewall XYZ** y vincularlo al OU **Member Servers XYZ**.

Member Servers FQM					
Objetos de directiva de grupo vinculados		Herencia de directivas de grupo	Delegación		
	Orden de vínculos	GPO	Exigido	Vínculo habilitado	Estado de GPO
	1	Member Server sec...	No	Sí	Habilitado
	2	Application Servers ...	No	Sí	Habilitado


17. Editar el GPO **Application Servers Firewall XYZ** y configurar las reglas del Firewall.

- En LON-DC1 editar el GPO **Application Servers Firewall**.
- Expandir **Configuración del equipo** -> **Directivas** -> **Configuración de Windows** -> **Configuración de seguridad** -> **Firewall de Windows con seguridad avanzada** -> **Firewall de Windows con seguridad avanzada – LDAP://CN={GUID}**.
- En **Reglas de entrada** crear una nueva regla con los siguientes parámetros:
 - Tipo de regla: Personalizada
 - Programa: Todos los programas
 - Tipo de protocolo: TCP
 - Puerto local: Puertos específicos -> 8080

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	18 / 21

- Ámbito: Cualquier dirección IP
- Acción: Permitir la conexión
- Perfil: Solo Dominio, no Privado ni Público.
- Nombre: Regla para Firewall XYZ

- Cerrar el editor de directivas.

Nombre	Grupo	Perfil	Habilitado	Acción	Invaldar
 Regla para firewall FQM		Domi...	Sí	Permitir	No

18. Limitar para que el GPO **Application Servers Firewall XYZ** solo se aplique al grupo **Application Server XYZ**.

- En LON-DC1 expandir el OU **Member Servers XYZ** y hacer clic en el GPO **Application Servers Firewall XYZ**.
- En el panel **Filtrado de seguridad** quitar todas las asignaciones y agregar el grupo **Application Servers XYZ**.


Application Servers Firewall FQM

Ámbito Detalles Configuración Delegación

Vínculos

Mostrar vínculos en esta ubicación:


Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado	Ruta
 Member Servers FQM	No	Sí	ACMEFQM.COM/Member Servers FQ

< >

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:


Nombre
 Application Servers FQM (ACMEFQM\Application Servers FQM)

Agregar... Quitar Propiedades

19. En LON-SVR-A iniciar como **Administrador** y ejecutar **gpupdate /force** para refrescar las directivas definidas previamente.

- Reiniciar el servidor e iniciar sesión como **Administrador**.

Entregable 4. Capture la pantalla donde se muestre el resultado del paso 19.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	19 / 21

```
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>gpupdate /force
Actualizando directiva...


La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

C:\Users\Administrador>_
```

20. Al finalizar el laboratorio, en el LON-DC1 deshacer los cambios realizados en el paso 1, es decir volver los objetos equipo al OU en donde se encontraban antes del inicio del laboratorio.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	20 / 21

4. EVALUACIÓN

		Administración de Redes y Comunicaciones				
		Rúbrica				
Resultado						
Criterio de desempeño						
Curso	Administración de Sistemas Operativos				Periodo	2020-1
Actividad	Seguridad en Servidores Windows usando GPOs				Semestre	III
Nombre del Alumno					Semana	8
Docente	Adriana Arista	Fecha	28/05/2020		Sección	A-B
Criterios a Evaluar		Excelente	Bueno	Requiere Mejora	No Aceptable	Puntaje Logrado
Configura GPO para asegurar servidores miembros del dominio.		4	3	2	0	
Crea auditorias para el acceso al sistema de archivos e inicios de sesión al dominio.		4	3	2	0	
Configura las políticas de AppLocker y el firewall de Windows		4	3	2	0	
Redacta correctamente los pasos principales de la implementación y conclusiones.		4	3	2	0	
Se comunica de manera efectiva, trabaja con orden, limpieza y puntualidad		4	3	2	0	
Total		20	15	10	0	

Comentarios respecto del desempeño del alumno	
---	--

	Descripción
Excelente	Demuestra un completo entendimiento del problema o realiza la actividad cumpliendo todos los requerimientos especificados.
Bueno	Demuestra un considerable entendimiento del problema o realiza la actividad cumpliendo con la mayoría de los requerimientos especificados.
Requiere Mejora	Demuestra un bajo entendimiento del problema o realiza la actividad con pocos de los requerimientos especificados.
No aceptable	No demuestra entendimiento del problema o actividad.

	LABORATORIO N°8 Seguridad en Servidores Windows usando GPOs	CÓDIGO:	TDG-TA-GUIA 08
		EMISION:	28/05/2020
		PAGINA:	21 / 21

5. CONCLUSIONES

- La vinculación de los Gpo se dan a un sitio, dominio o unidad organizativa , en el laboratorio que hemos realizado solo se da en el OU que hemos aplicado como tal
- Al momento de agregar grupos tenemos la posibilidad de no equivocarnos al hacer uso del botón Examinar, el cual busca por si solo solo con las iniciales que agregamos
- Podemos agregar los grupos como miembros de grupo predeterminado, o local para tener el acceso de administrador en donde sea que ingresemos
- Para la verificación de la aplicación de las configuraciones que se dan debemos de reinicarlo y a su vez forzar con el comando gpupdate /forcé, aunque a veces no se permita este comando no hay mejor forma que hacerlo que reiniciando ya que se trata de configuraciones en equipos
- Se reconoció el procedimiento y verificar que las directivas que estamos configurando son las que deben ser

6. ANEXOS (NO APLICA)