

Prueba - Supervisión y auditoría de servicios críticos en Windows Server

Integrantes:

Pablo Ulloa

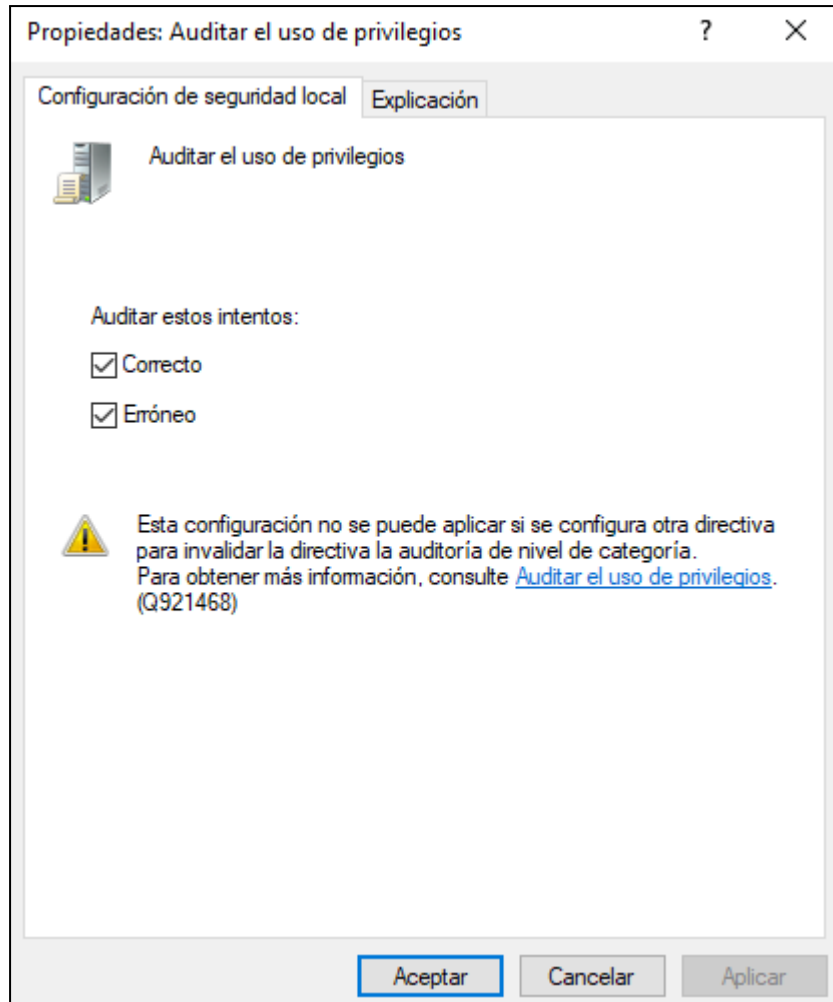
Gonzalo Yañez

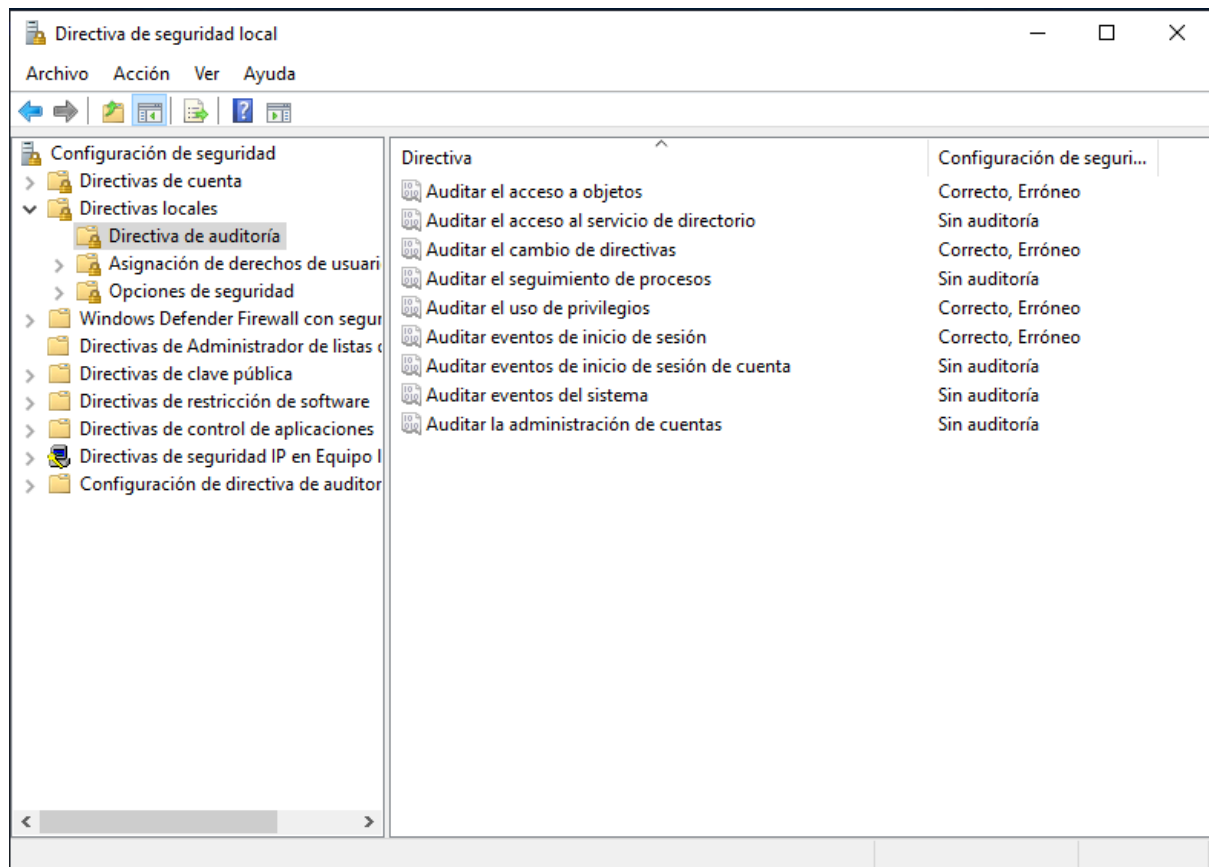
Helmo Velazquez

Macarena Quijada

1. Habilitación de auditoría de eventos críticos

- Configurar las Directivas de Seguridad Local para habilitar la auditoría de Eventos en Windows Server.





2. Monitoreo con Event Viewer y Sysmon

- Implementar Sysmon para el monitoreo avanzado de eventos de seguridad.

Instalar sysmon en el servidor.

```

PS C:\Users\Administrador> sysmon -c C:\Sysmon\sysmonconfig.xml
sysmon :
En línea: 1 Carácter: 1
+ sysmon -c C:\Sysmon\sysmonconfig.xml
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Configuration updated.
  
```

- Filtrar y analizar eventos relevantes relacionados con servicios críticos.

Eventos de creación de procesos sospechosos

```
PS C:\Users\Administrador> Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational -FilterXPath "[*][System/EventID=1]"

ProviderName: Microsoft-Windows-Sysmon

TimeCreated      Id LevelDisplayName Message
-----
01/07/2025 4:32:45 1 Información Process Create:...
01/07/2025 4:32:45 1 Información Process Create:...
01/07/2025 4:31:29 1 Información Process Create:...
01/07/2025 4:31:26 1 Información Process Create:...
01/07/2025 4:28:21 1 Información Process Create:...
01/07/2025 4:28:20 1 Información Process Create:...
01/07/2025 4:28:19 1 Información Process Create:...
01/07/2025 4:26:59 1 Información Process Create:...
01/07/2025 4:25:02 1 Información Process Create:...
01/07/2025 4:25:02 1 Información Process Create:...
```

Conexiones de redes inusuales

```
PS C:\Users\Administrador> Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational -FilterXPath "[*][System/EventID=3]"

ProviderName: Microsoft-Windows-Sysmon

TimeCreated      Id LevelDisplayName Message
-----
01/07/2025 6:08:08 3 Información Network connection detected:...
```

Filtrar registro actual

FiltroXML

Registrado:Última hora

Nivel del evento:

☒ Crítico

☒ Advertencia

☐ Detallado

☒ Error

☒ Información

☒ Por registro

Registros de eventos:Microsoft-Windows-Sysmon/Operational

☐ Por origen

Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

1,13,22

Categoría de la tarea:

Palabras clave:



















Usuario:<Todos los usuarios>

Equipo(s):<Todos los equipos>

Borrar

Aceptar

Cancelar

Operational Número de eventos: 507 (!) Nuevos eventos disponibles				
Filtrados:Registro: Microsoft-Windows-Sysmon/Operational; Niveles: Critico, Error, Advertencia, Información; Origen: ; Id. del evento: 13,22Intervalo de datos: Última hora.				
Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
 Información	01/07/2025 5:55:00	Sysmon	13	Registry value set (rule: RegistryEvent)
 Información	01/07/2025 5:55:00	Sysmon	13	Registry value set (rule: RegistryEvent)
 Información	01/07/2025 5:55:00	Sysmon	13	Registry value set (rule: RegistryEvent)
 Información	01/07/2025 5:55:00	Sysmon	13	Registry value set (rule: RegistryEvent)
 Información	01/07/2025 5:52:53	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:52:53	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:52:31	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:52:30	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:42	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:38	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:38	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:38	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:37	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:37	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:22	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:21	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:21	Sysmon	22	Dns query (rule: DnsQuery)
 Información	01/07/2025 5:51:21	Sysmon	22	Dns query (rule: DnsQuery)

● Profundizando Sysmon

Sysmon es una herramienta gratuita de Microsoft que se instala como un servicio en Windows para registrar eventos del sistema de bajo nivel, como:

- Creación de procesos
- Conexión de red
- Cambios en archivos
- Acceso a registros
- Carga de drivers

Objetivo principal: Ayudar a detectar actividad sospechosa, malware, movimiento lateral, persistencia, etc.

¿Cómo funciona?

Se ejecuta como servicio persistente en segundo plano, registrando en el Visor de eventos de Windows:

Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

Tipos de eventos comunes

ID	Evento	Descripción breve
1	Process Create	Proceso iniciado, con ruta, hash, PID, usuario, argumentos.
3	Network Connection	Conexión de red saliente (IP, puerto, proceso).
5	Process Terminate	Proceso finalizado.
6	Driver Loaded	Driver cargado en el sistema.
7	Image Loaded	Librería DLL cargada.
8	CreateRemoteThread	Indicador de inyección de código.
11	File Create	Archivo creado.
13	Registry Value Set	Modificación en el registro.
15	FileStream Detected	Escritura de flujo alternativo (ADS).
22	DNS Query	Consulta DNS realizada por un proceso.

¿Por qué usar Sysmon?

Alta visibilidad	Registra eventos que el visor de eventos normal no muestra.
Bajo impacto	Muy liviano, ideal para producción.
Detección de amenazas	Aporta evidencia para detectar malware, ransomware, etc.

3. Análisis de registros de auditoría

- Examinar los registros obtenidos y detectar patrones sospechosos o anómalos.

Visor de Eventos

Seguridad Número de eventos: 7.975 (!) Nuevos eventos disponibles					
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea	
Error de auditoría	02/07/2025 6:22:36	Microsoft Windows securit...	5152	Filtering Platform Packet ...	
Error de auditoría	02/07/2025 6:22:36	Microsoft Windows securit...	5152	Filtering Platform Packet ...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5156	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5156	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5158	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5158	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	4634	Logoff	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	4627	Group Membership	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	4672	Special Logon	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5156	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5156	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:44	Microsoft Windows securit...	5158	Filtering Platform Connec...	
Error de auditoría	02/07/2025 6:21:43	Microsoft Windows securit...	5152	Filtering Platform Packet ...	
Error de auditoría	02/07/2025 6:21:43	Microsoft Windows securit...	5152	Filtering Platform Packet ...	
Auditoría correcta	02/07/2025 6:21:04	Microsoft Windows securit...	5156	Filtering Platform Connec...	
Auditoría correcta	02/07/2025 6:21:04	Microsoft Windows securit...	5156	Filtering Platform Connec...	

Inicio de Sesión Fallida (4625)

Seguridad Número de eventos: 1.276					
Filtros:Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4625Intervalo de datos: Última hora. Número de eventos: 4					
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea	
Error de auditoría	02/07/2025 5:29:14	Microsoft Windows securit...	4625	Logon	
Error de auditoría	02/07/2025 5:29:12	Microsoft Windows securit...	4625	Logon	
Error de auditoría	02/07/2025 5:29:10	Microsoft Windows securit...	4625	Logon	
Error de auditoría	02/07/2025 5:29:07	Microsoft Windows securit...	4625	Logon	

Inicio de Sesión Correcta (4624)

Seguridad Número de eventos: 1.796					
Filtros:Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4624Intervalo de datos: Última hora. Número de eventos: 46					
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea	
Auditoría correcta	02/07/2025 5:34:09	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 5:33:07	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 5:33:07	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 5:32:56	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 5:32:55	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 5:32:55	Microsoft Windows securit...	4624	Logon	
Auditoría correcta	02/07/2025 5:32:55	Microsoft Windows securit...	4624	Logon	

Acceso a un archivo u objeto (4663)

Seguridad Número de eventos: 1.986					
Filtros:Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4663Intervalo de datos: Última hora. Número de eventos: 1					
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea	
Auditoría correcta	02/07/2025 5:28:45	Microsoft Windows securit...	4663	Kernel Object	

Cambios en directivas de auditoría (4719)

Seguridad Número de eventos: 4.009				
Filtros:Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4719Intervalo de datos: Última hora. Número de eventos: 36				
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:49	Microsoft Windows securit...	4719	Audit Policy Change
Auditoría correcta	02/07/2025 5:41:43	Microsoft Windows securit...	4719	Audit Policy Change

Creación de nueva cuenta (4720)

Seguridad Número de eventos: 4.876				
Filtros:Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4720. Número de eventos: 2				
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	02/07/2025 5:48:34	Microsoft Windows securit...	4720	User Account Management
Auditoría correcta	02/07/2025 5:48:13	Microsoft Windows securit...	4720	User Account Management

Intento de cambio de contraseña (4723)

Seguridad Número de eventos: 6.553				
Filtros:Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4723. Número de eventos: 1				
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	02/07/2025 5:57:32	Microsoft Windows securit...	4723	User Account Management

Evento 4723, Microsoft Windows security auditing.

General	Detalles
Sujeto:	
Id. de seguridad:	ENTERPRISE\jperes
Nombre de cuenta:	jperes
Dominio de cuenta:	ENTERPRISE
Id. de inicio de sesión:	0x45F09D
Cuenta de destino:	
Id. de seguridad:	ENTERPRISE\jperes
Nombre de cuenta:	jperes
Dominio de cuenta:	ENTERPRISE

Eliminación de cuenta (4726)

Seguridad Número de eventos: 6.846

Filtros: Registro: Security; Niveles: Crítico, Error, Advertencia, Información, Detallado; Origen: ; Id. del evento: 4720. Número de eventos: 2

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	02/07/2025 5:48:34	Microsoft Windows securit...	4720	User Account Management
Auditoría correcta	02/07/2025 5:48:13	Microsoft Windows securit...	4720	User Account Management

Evento 4720, Microsoft Windows security auditing.

General Detalles

Sujeto:

Id. de seguridad:	ENTERPRISE\Administrador
Nombre de cuenta:	Administrador
Dominio de cuenta:	ENTERPRISE
Id. de inicio de sesión:	0x30D03A

Nueva cuenta:

Id. de seguridad:	S-1-5-21-370996450-4123769158-3727965300-1105
Nombre de cuenta:	scea
Dominio de cuenta:	ENTERPRISE

4. Implementación de alertas de seguridad

- Configurar alertas en el Visor de Eventos para recibir notificaciones sobre actividades sospechosas.

Se programara una tarea para que detecte eventos importante ocurriendo dentro del servidor, estos eventos tienen los siguientes ID 's.


4728 – Se agregó un miembro a un grupo.

4729 – Se eliminó un miembro de un grupo.

4732 – Se agregó un miembro a un grupo privilegiado.

4733 – Se eliminó un miembro de un grupo privilegiado.

Asistente para crear tareas básicas

 Cuando se registre un evento específico

Crear una tarea básica

Al registrar un evento

Acción

Finalizar


Registro: Seguridad

Origen:

Id. del evento:

< Atrás Siguiete > Cancelar

Asistente para crear tareas básicas

 Acción

Crear una tarea básica

Al registrar un evento

Acción

Finalizar

¿Qué acción desea que realice la tarea?


☒ Iniciar un programa

☐ Enviar un correo electrónico (desusado)

☐ Mostrar un mensaje (desusado)

< Atrás Siguiete > Cancelar

Asistente para crear tareas básicas

 Iniciar un programa

Crear una tarea básica

Al registrar un evento

Acción

Iniciar un programa

Finalizar

Programa o script: powershell.exe -File C:\Scripts\AD_Alert.ps1


Examinar...

Agregar argumentos (opcional):

Iniciar en (opcional):

< Atrás Siguiete > Cancelar

Asistente para crear tareas básicas

 Resumen

Crear una tarea básica

Al registrar un evento

Acción

Iniciar un programa

Finalizar

Nombre: Monitoreo eventos importantes

Descripción: IDs supervisadas: 4728, 4729, 4732 y 4733.

Desencadenador: Al producirse un evento; Al producirse un evento - Registro: Security

Acción: Iniciar un programa; powershell.exe -File C:\Scripts\AD_Alert.ps1

☐ Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar

Al hacer clic en Finalizar, la nueva tarea se creará y se agregará a su programación de Windows.

< Atrás Finalizar Cancelar

Crear Script "AD_Alert.ps1".


```

AD_Alert.ps1 X
1 # Ruta del archivo de log
2 $logPath = "C:\Scripts\Alerta_Eventos_Sospechosos.log"
3
4 # Fecha y hora
5 $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
6
7 # Mensaje
8 $mensaje = "$timestamp - ACTIVIDAD SOSPECHOSA: Se detectó un evento crítico de seguridad"
9
10 # Registrar en archivo
11 Add-Content -Path $logPath -Value $mensaje
12
13 # Mostrar alerta en pantalla (si es escritorio y no servidor core)
14 [System.Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms")
15 [System.Windows.Forms.MessageBox]::Show("Actividad sospechosa detectada. Revisar los registros.", "Alerta de Seguridad", 0, [System.Windows.Forms.Me

```

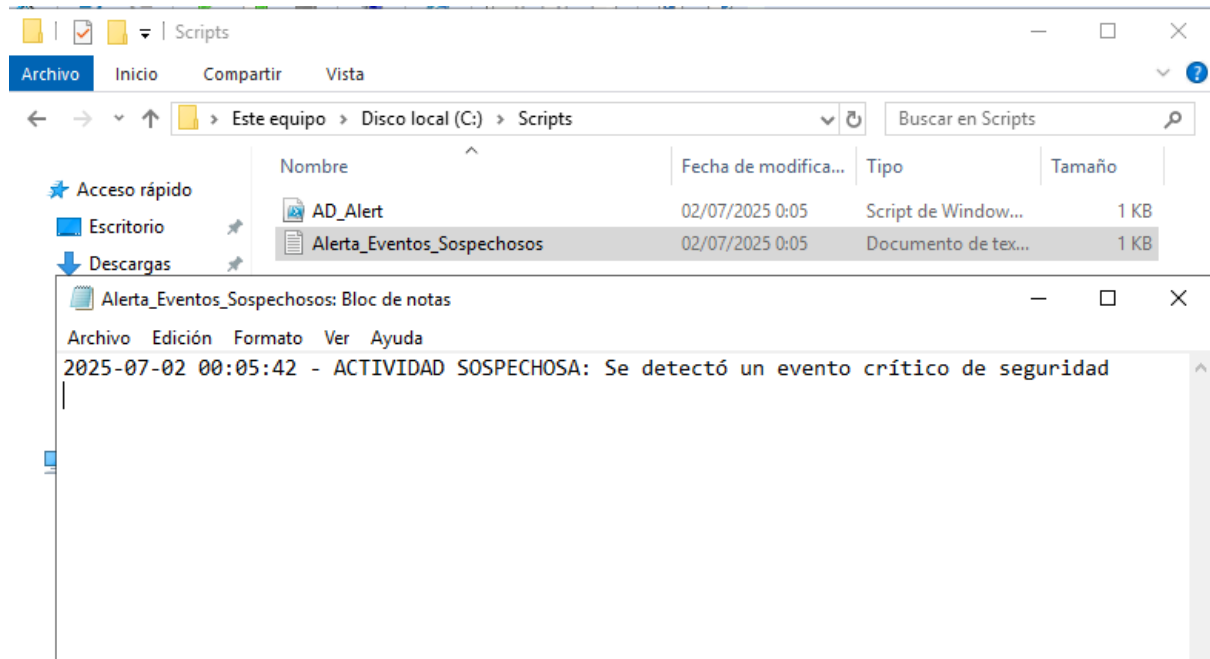
Genera el siguiente mensaje cada vez que se detecta uno de los eventos indicados.

Alerta de Seguridad

 Actividad sospechosa detectada. Revisar los registros.

Aceptar

Creando un Log con más detalles e información.



5. Recomendaciones y plan de mejora

- Proponer al menos 3 mejoras en la configuración de seguridad basadas en los hallazgos del monitoreo.

1. Implementar AppLocker para restringir la ejecución de software no autorizado.

Durante el monitoreo con Sysmon (ver punto 2), se detectaron múltiples procesos ejecutados desde ubicaciones no estándar, lo que representa un riesgo potencial de ejecución de código malicioso. Como medida preventiva, se propone la implementación de AppLocker para limitar la ejecución únicamente a binarios firmados digitalmente o ubicados en carpetas confiables (como C:\Program Files). Esto evitará que los usuarios ejecuten scripts o aplicaciones desde rutas como el escritorio o la carpeta Temp.

Además, se recomienda aplicar esta política primero en modo auditoría para evaluar su impacto antes de aplicarla de forma restrictiva.

2. Establecer límites de intentos fallidos de inicio de sesión mediante directivas de cuenta.

El análisis del Visor de Eventos (punto 3) reveló múltiples intentos de inicio de sesión, lo que podría indicar un ataque de fuerza bruta. Para prevenir accesos no autorizados, se recomienda configurar las directivas de cuenta en secpol.msc para limitar los intentos fallidos:

Número máximo de intentos fallidos: 3

Bloqueo de cuenta: 15 minutos

Reinicio del contador: cada 15 minutos

Estas configuraciones aumentan significativamente la dificultad de ataques de tipo fuerza bruta, y funcionan como medida preventiva de bajo impacto y alta efectividad.

También se recomienda revisar los eventos 4625 (inicio fallido) y 4624 (inicio exitoso) regularmente.

3. Implementar autenticación multifactor (MFA) para cuentas administrativas en Azure AD.

Durante la simulación (punto 3), se detectó un intento de cambio de contraseña en una cuenta administrativa, lo que representa un riesgo elevado si la cuenta ha sido comprometida o su contraseña ha sido filtrada. Para reforzar el control de acceso, se propone habilitar MFA en Azure Active Directory para todas las cuentas con privilegios elevados.

Esto añade una segunda capa de verificación (como una app móvil o código SMS), lo que previene accesos no autorizados incluso si la contraseña ha sido robada.

Esta es una medida preventiva, recomendada por estándares como NIST y CIS Benchmarks, y puede implementarse desde el portal de Azure AD > Seguridad > Autenticación multifactor.