REPORTE DE LOGS

Fecha y Hora	Tipo de Evento	Usuario Implicado	Objeto/Proceso	Descripción/Mensaje del Log	Resolución/Implicación

19/06/2025 10:15	Login Fallido	UsuarioInvalido	Inicio de Sesión	"An account failed to log on.
				Subject:
				  Security ID: SID_NULL
				  Account Name: UsuarioInvalido
				  Account Domain: WORKGROUP
				 Logon Type: 2
				 Failure Reason: Unknown user name or bad password.
				 Status: 0xC000006D
				 Sub Status: 0xC000006A"
					Indica un intento no autorizado de acceso al sistema con credenciales incorrectas. Podría ser un error tipográfico o un intento de ataque de fuerza bruta/adivinación de contraseñas. Requiere monitoreo continuo.

19/06/2025 10:16	Login Fallido	Administrador	Inicio de Sesión	"An account failed to log on.
				Subject:
				  Security ID: SID_NULL
				  Account Name: Administrador
				  Account Domain: LOCALHOST
				 Logon Type: 10
				 Failure Reason: Account currently locked out.
				 Status: 0xC0000234
				 Sub Status: 0x0"
					El intento de inicio de sesión falló debido a que la cuenta Administrador está bloqueada, probablemente por múltiples intentos fallidos anteriores. Esto es una medida de seguridad activa contra ataques de fuerza bruta.

Fecha y Hora	Tipo de Evento	Usuario Implicado	Objeto/Proceso	Descripción/Mensaje del Log	Resolución/Implicación

19/06/2025 10:30	Acceso a Recurso Denegado	UsuarioA	Archivo: C:\MiEmpresa\Finanzas\Presupuesto.xlsx	"An attempt was made to access an object.
				 Subject:
				  Security ID: DESKTOP-LAB\UsuarioA
				  Account Name: UsuarioA
				  Account Domain: DESKTOP-LAB
				 Object:
				  Object Server: Security
				  Object Type: File
				  Object Name: C:\MiEmpresa\Finanzas\Presupuesto.xlsx
				 Access Request: WriteData (denied)"
					El usuario UsuarioA intentó modificar un archivo en la carpeta "Finanzas" y el acceso fue denegado debido a los permisos establecidos (solo lectura o sin permisos de escritura). Esto confirma que las políticas de control de acceso funcionan correctamente para proteger datos sensibles.

19/06/2025 10:31	Acceso a Recurso Denegado	UsuarioB	Carpeta: C:\MiEmpresa\RecursosHumanos	"An attempt was made to access an object.
				 Subject:
				  Security ID: DESKTOP-LAB\UsuarioB
				  Account Name: UsuarioB
				  Account Domain: DESKTOP-LAB
				 Object:
				  Object Server: Security
				  Object Type: Directory
				  Object Name: C:\MiEmpresa\RecursosHumanos
				 Access Request: ListDirectory (denied)"
					El usuario UsuarioB intentó listar el contenido de la carpeta "RecursosHumanos" sin los permisos adecuados. Esto valida la segregación de acceso a información confidencial del departamento de RRHH.

Fecha y Hora	Tipo de Evento	Usuario Implicado	Objeto/Proceso	Descripción/Mensaje del Log	Resolución/Implicación

19/06/2025 10:45	Cambio de Política de Auditoría	SYSTEM	Directiva de Auditoría	"Auditing settings on object were changed.
				 Subject:
				  Security ID: SYSTEM
				  Account Name: DESKTOP-LAB$
				 Object Type: File
				 Object Name: C:\Windows\System32\audit.dll
				 Auditing Settings: S:AINO_ACCESS_CONTROL -> S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)"
					El sistema modificó las configuraciones de auditoría en un objeto del sistema (probablemente a raíz de una actualización o un cambio manual de configuración de seguridad). Es importante monitorear estos eventos para detectar intentos de deshabilitar la auditoría o modificarla con fines maliciosos.

19/06/2025 10:50	Enumeración de Grupo Local	CSIRT	Grupo: Administradores	"A user's local group membership was enumerated.
				 Subject:
				  Security ID: DESKTOP-LAB\CSIRT
				  Account Name: CSIRT
				  Account Domain: DESKTOP-LAB
				 User:
				  Security ID: DESKTOP-LAB\CSIRT
				  Account Name: CSIRT
				 Process Name: C:\Windows\System32\mmc.exe"
					El usuario CSIRT enumeró la membresía de un grupo local (posiblemente a través de la consola de "Administración de equipos"). Este evento es normal para usuarios con roles de seguridad o administración, pero una enumeración inesperada por un usuario no autorizado podría indicar reconocimiento de objetivos para un ataque.

19/06/2025 11:05	Proceso Terminando	SYSTEM	Proceso: notepad.exe (PID: 1234)	"An attempt was made to terminate a process.
				 Subject:
				  Security ID: SYSTEM
				  Account Name: DESKTOP-LAB$
				 Process ID: 0x1234
				 Process Name: C:\Windows\System32\notepad.exe
				 Termination Reason: Process exited normally"
					Un proceso del sistema (notepad.exe) ha terminado su ejecución de forma normal. Estos eventos son comunes, pero un patrón de terminaciones inesperadas o forzadas de procesos críticos podría indicar actividad maliciosa o inestabilidad del sistema.

Conclusión del Reporte de Eventos de Seguridad

El análisis de los logs de seguridad es una actividad fundamental para cualquier estrategia de ciberseguridad. Permite identificar intentos de acceso no autorizado, evaluar la efectividad de las políticas de permisos y detectar actividades sospechosas que podrían indicar una brecha de seguridad. La capacidad de correlacionar eventos de diferentes fuentes (autenticación, acceso a objetos, sistema, aplicaciones) proporciona una visión integral de la postura de seguridad del entorno. Un monitoreo proactivo y una respuesta rápida a los eventos críticos son esenciales para mantener la resiliencia del sistema frente a amenazas.