Plan de Monitorización y Logging

Tabla de contenidos

1 Objetivo

El presente plan establece las directrices y procedimientos para la recolección, centralización, supervisión y análisis de eventos de seguridad en la infraestructura tecnológica de la sede de Barcelona. Su propósito es garantizar la trazabilidad de acciones relevantes, permitir la detección temprana de amenazas, cumplir con requisitos legales y normativos, y facilitar el análisis forense en caso de incidentes.

2 Alcance

Este plan aplica a todos los sistemas informáticos, redes, dispositivos de seguridad y servicios desplegados en la sede de Barcelona. Incluye tanto sistemas locales como aquellos integrados mediante conectividad VPN con la sede central (Madrid) y recursos en la nube.

Los elementos cubiertos incluyen:

- Firewalls locales (NGFW).
- Conmutadores gestionables (VLANs segmentadas).
- Servidores físicos y virtualizados.
- Plataformas de almacenamiento de archivos y proyectos.
- Centralita y telefonía integrada.
- Estaciones de trabajo y portátiles corporativos.
- Sistemas de autenticación (LDAP, VPN con MFA).
- Infraestructura de cifrado y certificados digitales (PKI).
- Accesos remotos y servicios VPN corporativos.
- Conectividad con recursos en la nube.

3 Referencias Normativas

- ISO 27001:2013 – A.12.4 Registro de actividades
- ISO 27002 – A.12.4.1 a A.12.4.3
- MAGERIT v3.0 – Análisis y trazabilidad de riesgos
- NIST SP 800-53 Rev.5 – AU-2 a AU-6, AU-12
- Reglamento General de Protección de Datos (RGPD)
- Reglamento LOPDGDD (España)

4 Fuentes de Logging

La siguiente tabla resume los activos críticos monitorizados en la sede y los tipos de eventos registrados:

Fuente	Tipo de eventos	Finalidad del registro
Firewall NGFW (local)	Conexiones entrantes/salientes, tráfico anómalo, accesos denegados, reglas aplicadas	Control del perímetro, detección de intrusiones
Virtualización	Logs de hipervisor, encendido/apagado de máquinas, cambios de red virtual	Seguimiento de servidores virtuales y su seguridad
Servidor local de backup	Copias realizadas, errores de sincronización, restauraciones	Validación de estrategia de respaldo y DRP
Active Directory (remoto)	Autenticaciones, cambios de grupo, políticas aplicadas	Control de identidades centralizado
VPN corporativa	Conexiones activas, fallos de MFA, IP origen	Control de acceso remoto seguro
Centralita	Actividad de softphones, acceso por app, llamadas SIP	Supervisión de telefonía y calidad del servicio
Bases de datos internas	Accesos privilegiados, consultas masivas, errores de integridad	Protección de información crítica y cumplimiento RGPD
Estaciones de trabajo	Logins, ejecución de software no autorizado, eventos críticos del sistema	Prevención de incidentes por endpoints

5 Tipología de Eventos a Registrar

De forma obligatoria, se registrarán y analizarán los siguientes eventos:

- Autenticaciones exitosas y fallidas (VPN, LDAP, aplicaciones).
- Accesos fuera del horario habitual.
- Elevaciones de privilegio o uso de cuentas administrativas.
- Cambios en configuraciones de red, firewall o cifrado.
- Manipulación de archivos sensibles.
- Transferencias de grandes volúmenes de datos.
- Descarga o transferencia de datos sensibles o críticos.
- Detección de malware o comportamiento sospechoso.
- Conexiones desde ubicaciones geográficas no habituales.

6 Clasificación y Severidad

Los eventos se clasifican para priorizar su análisis:

- **Críticos**: accesos no autorizados, elevación de privilegios, malware activo, cambios en firewalls.
- **Altos**: múltiples intentos de login fallidos, escaneo de puertos detectado.
- **Medios**: cambios en contraseñas, actualización de certificados.
- **Bajos**: información de sistema, eventos rutinarios.

7 Recolección y Almacenamiento

7.1 Centralización

Todos los eventos relevantes son reenviados en tiempo real al **sistema SIEM corporativo** alojado en la sede de Madrid. La transmisión se realiza cifrada (TLS 1.3) y autenticada. En caso de pérdida de conectividad, los logs son almacenados localmente hasta su retransmisión segura.

7.2 Integridad y Retención

- Los registros son firmados digitalmente para garantizar su integridad.
- La retención mínima es de **1 año** para eventos comunes, y hasta **5 años** para incidentes o eventos vinculados a datos personales o de auditoría.

8 Supervisión y Revisión

El equipo de Seguridad TI realiza:

- Revisión diaria de eventos críticos en el SIEM.
- Monitoreo en tiempo real de alertas automatizadas por correlación de eventos.
- Informes semanales de actividad anómala enviados a la Dirección de TI.
- Revisión mensual de los dispositivos no integrados o con errores de transmisión.

9 Alertas Automáticas

Se han definido alertas inmediatas para los siguientes escenarios:

- Accesos administrativos desde IP externas.
- Fallos repetidos en autenticación VPN.
- Instalación no autorizada de software.
- Desactivación de antivirus o pérdida de conexión con EDR.
- Cambio en políticas de firewall o eliminación de reglas activas.

Las alertas son notificadas vía correo electrónico y Teams al equipo de seguridad.

10 Responsabilidades

Rol	Funciones asignadas
Administrador de seguridad	Gestión del SIEM, análisis de eventos críticos.
Técnicos de red/sistemas	Configuración de logging, transmisión segura, revisión de dispositivos.
Responsable de cumplimiento	Validación del plan frente a normativa (RGPD).
Auditores internos	Evaluación del cumplimiento, revisión de logs históricos y trazabilidad.

11 Evaluación y Actualización

- Este plan será revisado **anualmente** o tras cualquier incidente significativo.
- Se documentarán todas las modificaciones, pruebas de eficacia y hallazgos de auditoría que deriven en ajustes del sistema de logging.
- Se incluye dentro del plan de auditoría y forma parte del control A.12.4 en el marco ISO 27001.