					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P22					Título del documento: **Política de registro y supervisión**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

1. Propósito

1.1 El propósito de esta política es establecer requisitos claros y exigibles para la generación, protección, revisión y análisis de registros que capturen eventos clave de auditoría del sistema y de seguridad en todo el entorno de TI de la organización.

1.2 El registro de eventos y la supervisión son fundamentales para la detección de anomalías, la respuesta ante amenazas, la investigación forense, la preparación para auditorías y el cumplimiento legal. Esta política garantiza que todos los eventos generados por los sistemas se registren, conserven y correlacionen adecuadamente, con precisión sustentada en registros con sincronización horaria.

1.3 Esta política es esencial para dar soporte a la cláusula 8.1 de ISO/IEC 27001 y a los controles 8.15 (registro de eventos), 8.16 (supervisión) y 8.17 (sincronización de relojes) del anexo A, y se vincula directamente con las obligaciones regulatorias del RGPD de la UE, la Directiva NIS2 de la UE, DORA de la UE y COBIT 2019.

2. Alcance

2.1 Esta política se aplica a todos los sistemas, servicios y entornos que almacenan, tratan o transmiten datos cubiertos por el Sistema de Gestión de la Seguridad de la Información (SGSI), incluidos:

2.1.1 Infraestructura local, servicios en la nube (p. ej., IaaS, PaaS, SaaS) y entornos híbridos

2.1.2 Sistemas operativos, bases de datos, aplicaciones y dispositivos de red

2.1.3 Sistemas de seguridad como SIEM, cortafuegos, plataformas de detección y respuesta en endpoints (EDR), concentradores VPN y proveedores de identidad

2.2 Las siguientes partes interesadas están incluidas en el alcance:

2.2.1 Usuarios internos con privilegios de sistema o administrativos

2.2.2 Personal de infraestructura y operaciones de TI

2.2.3 Centro de Operaciones de Seguridad (SOC) y equipos de detección de amenazas

2.2.4 Desarrolladores de software y propietarios de aplicaciones

2.2.5 Proveedores de servicios externos que gestionan sistemas que generan registros

3. Objetivos

3.1 Garantizar que todos los sistemas críticos generen registros de eventos de seguridad y registros de actividad del sistema, y que estos se conserven de conformidad con los requisitos regulatorios, legales y contractuales.

3.2 Definir los tipos mínimos de eventos y el contenido de registro necesarios para detectar actividades no autorizadas, trazar las acciones de los usuarios y dar soporte a las investigaciones forenses.

3.3 Aplicar medidas de protección para evitar la manipulación de registros, su eliminación no autorizada o el acceso no controlado a los datos de registro.

3.4 Establecer sistemas centralizados de registro de eventos y alertas (p. ej., SIEM) para agregar, correlacionar y escalar actividad sospechosa en tiempo casi real.

3.5 Garantizar la sincronización de los relojes de los sistemas para permitir una correlación precisa entre sistemas y el análisis de incidentes.

3.6 Facilitar la mejora continua y el cumplimiento mediante la integración de la supervisión de registros con los procesos de auditoría, gestión de riesgos y gestión de incidentes.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de esta política y garantiza su alineación con la postura de riesgo de la organización, los requisitos de auditoría y las obligaciones del SGSI.

4.1.2 Aprueba el alcance del registro de eventos para sistemas regulados o de alto riesgo y supervisa los informes de cumplimiento.

4.2 Responsable del Centro de Operaciones de Seguridad (SOC)

4.2.1 Opera y mantiene las plataformas centralizadas de gestión de registros (p. ej., SIEM).

4.2.2 Define las reglas de agregación de registros, los umbrales de alerta y las vías de escalado para el triaje de incidentes.

4.2.3 Revisa los informes diarios y garantiza que las anomalías se analicen, documenten y escalen cuando sea necesario.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política debe revisarse anualmente, o antes en respuesta a:

9.1.1 Cambios significativos en la arquitectura de sistemas o en la infraestructura de registro (p. ej., migración de SIEM)

9.1.2 Revisiones de los requisitos regulatorios de registro (p. ej., mandatos de registro de NIS2 o DORA)

9.1.3 Hallazgos de auditorías o revisiones posteriores a incidentes

9.1.4 Amenazas emergentes que requieran una mayor supervisión (p. ej., amenazas internas, compromiso de la cadena de suministro)

9.2 El proceso de revisión será dirigido por el Responsable del Centro de Operaciones de Seguridad (SOC), en coordinación con el CISO, Gestión de Riesgos, Cumplimiento y los equipos de Infraestructura de TI.

9.3 Los cambios aprobados deben quedar sujetos a control de versiones en el Registro de Control Documental del SGSI y comunicarse a:

9.3.1 Todas las partes interesadas responsables del mantenimiento de los sistemas de registro

9.3.2 Los propietarios de aplicaciones y sistemas

9.3.3 Los proveedores externos con responsabilidades de telemetría o integración con SIEM

9.4 Todas las versiones sustituidas deben archivarse de forma segura, con acceso restringido a los custodios autorizados del SGSI para fines de auditoría y legales.

10. Políticas relacionadas y vinculaciones

10.1 P1 – Política de Seguridad de la Información. Establece el compromiso fundamental de proteger sistemas y datos, en cuyo marco el registro de eventos y la supervisión actúan como capacidades críticas de detección y respuesta.

10.2 P4 – Política de Control de Acceso. Garantiza que el acceso privilegiado, los inicios de sesión de usuarios y los eventos de autorización queden registrados y supervisados para detectar abusos o comportamientos anómalos.

10.3 P5 – Política de gestión de cambios. Exige el registro de cambios del sistema, despliegues de parches y actualizaciones de configuración que puedan introducir riesgos o modificaciones no autorizadas.

10.4 P21 – Política de seguridad de red. Requiere registro a nivel de red (p. ej., registros de cortafuegos, alertas de IDS/IPS, actividad VPN) e integración con SIEM para proporcionar visibilidad sobre anomalías del tráfico y la defensa perimetral.

10.5 P23 – Política de sincronización horaria. Exige coherencia horaria entre sistemas, lo cual es esencial para un registro fiable y la correlación de eventos de seguridad en múltiples entornos.

10.6 P30 – Política de Respuesta a Incidentes. Se basa en los datos de registro y en los mecanismos de alerta para identificar, investigar y responder a incidentes de seguridad, preservando además artefactos forenses para su revisión posterior al incidente.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Planificación y control operacional: exige controles para supervisar las operaciones y salvaguardar frente a accesos no autorizados y uso indebido de los sistemas.

11.2 ISO/IEC 27002:2022 – Controles 8.15, 8.16, 8

11.2.1 Define requisitos detallados de registro, incluidos qué eventos deben registrarse, cómo proteger y analizar los registros y cómo garantizar la fiabilidad de las marcas temporales entre sistemas.

11.3 NIST SP 800-53 Rev.

11.3.1 AU-2 a AU-12: abarca la selección de eventos, el registro, la protección, la revisión de auditoría, la respuesta ante fallos de auditoría y la conservación de registros de auditoría.

11.3.2 SI-4 – Supervisión del sistema: exige supervisión activa del sistema con alertas basadas en actividad anómala.

11.3.3 SC-45 – Sincronización horaria del sistema: refuerza la exactitud temporal para la trazabilidad de eventos y la correlación de incidentes.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 32 – Seguridad del tratamiento: exige controles técnicos como el registro y la supervisión para garantizar la seguridad y la responsabilidad proactiva, especialmente respecto del acceso a datos personales.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(e): exige sistemas de registro y supervisión de eventos para la detección y respuesta rápidas ante incidentes de seguridad.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 9 – Gestión del riesgo de las TIC: exige mecanismos para detectar actividad anómala, registrar incidentes y conservar datos forenses.

11.6.2 Artículo 11 – Pruebas de los Planes de Continuidad del Negocio (BCP/DRP) de TIC: hace hincapié en mantener la supervisión y validar la disponibilidad de registros durante interrupciones operativas.

11.7 COBIT 2019

11.7.1 DSS01.05 – Gestionar los registros de los servicios de seguridad: exige la implantación de capacidades de registro para toda la infraestructura crítica.

11.7.2 DSS05.04 – Supervisar eventos de seguridad: exige supervisión y análisis de registros en tiempo real para detectar y responder a eventos.

11.7.3 MEA03 – Supervisar, evaluar y valorar el cumplimiento: exige la revisión periódica de las prácticas de registro y su alineación con los objetivos de control.