					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P22S					Título del documento: **Política de registro de eventos 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**

Alineación con normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Controles operativos, incluido el registro de eventos
ISO/IEC 27002:2022	Controles 8.15, 8.16, 8.17	Registro de eventos, protección y supervisión
NIST SP 800-53 Rev.5	AU-2 a AU-12, SI-4	Contenido y revisión del registro de auditoría, conservación, detección de anomalías y alertas
RGPD de la UE	Artículos 5(1)(f), 32, 33	Confidencialidad e integridad de los datos, medidas técnicas y notificación de violaciones de seguridad de los datos personales
Directiva NIS2 de la UE	Artículos 21(2)(d), 23	Mecanismos de registro para anomalías y notificación de incidentes en un plazo de 24 h
DORA de la UE	Artículos 10, 15	Resiliencia operativa, supervisión y registro de eventos de proveedores de servicios
COBIT 2019	DSS01.03, DSS05.02	Trazabilidad de la actividad y protección mediante registro de eventos y supervisión

1. Propósito

1.1 Esta política establece controles obligatorios de registro de eventos y supervisión para garantizar la seguridad, la rendición de cuentas y la integridad operativa de los sistemas de TI de la organización.

1.2 Define los tipos de eventos que deben registrarse, cómo deben almacenarse los registros, cómo deben revisarse y las responsabilidades del personal y de los proveedores de servicios.

1.3 El registro de eventos y la supervisión respaldan la detección de amenazas, el cumplimiento normativo, la respuesta a incidentes y el análisis forense.

1.4 Esta política permite a la organización cumplir los requisitos de control operativo de ISO/IEC 27001 y respalda la preparación para auditorías, la confianza de los clientes y el cumplimiento del RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

2. Alcance

2.1 Esta política se aplica a todos los sistemas y usuarios de la organización, incluidos:

2.1.1 Estaciones de trabajo, equipos portátiles, servidores, cortafuegos, conmutadores, enrutadores y puntos de acceso inalámbrico

2.1.2 Servicios en la nube utilizados para las operaciones de la organización (p. ej., correo electrónico, almacenamiento de archivos, copias de seguridad y herramientas de colaboración)

2.1.3 Funciones de registro en software antivirus, aplicaciones, sistemas operativos y equipos de red

2.1.4 Todos los empleados, contratistas y proveedores de servicios gestionados (MSP) que utilicen o administren sistemas

2.1.5 Cualquier ubicación en la que se utilicen los sistemas de TI de la empresa, incluidos entornos remotos, híbridos o de traiga su propio dispositivo (BYOD)

2.2 La política también se aplica a los registros generados por servicios de terceros cuando la organización disponga de acceso administrativo o derechos contractuales de auditoría.

3. Objetivos

3.1 Garantizar el registro de la actividad del sistema, incluida la autenticación, los cambios de configuración, el acceso a datos sensibles y las alertas de seguridad

3.2 Mantener registros seguros y precisos para detectar incumplimientos de la política, errores del sistema o acciones no autorizadas

3.3 Permitir la revisión rápida de los registros durante incidentes, investigaciones y auditorías

3.4 Respaldar la sincronización horaria para garantizar la integridad y la correlación de los datos de registro

3.5 Proteger los registros frente a manipulaciones, pérdida o eliminación prematura

3.6 Cumplir las obligaciones regulatorias y legales relativas a la rendición de cuentas del sistema, la trazabilidad y la respuesta ante violaciones de seguridad

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba esta política y garantiza su implantación en todos los sistemas de la organización

4.1.2 Revisa las alertas de alta gravedad y los hallazgos graves de auditoría comunicados por TI o por las funciones de privacidad

4.1.3 Aprueba las excepciones cuando el registro o la conservación no puedan aplicarse técnicamente

4.2 Proveedor de soporte de TI / Función interna de TI

4.2.1 Implanta y configura el registro en sistemas operativos, dispositivos de red, herramientas antivirus y aplicaciones clave

4.2.2 Garantiza que los registros se conserven, se respalden y estén protegidos frente a alteraciones

4.2.3 Revisa los registros conforme a una programación establecida e investiga actividades sospechosas o no autorizadas

4.2.4 Mantiene sistemas de alerta que identifiquen comportamientos anómalos o indicadores de intrusión

[... 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 Revisión anual

9.1.1 Esta política debe revisarse al menos una vez al año por el Director General con el apoyo del Proveedor de soporte de TI y del Coordinador de Privacidad.

9.2 Desencadenantes de revisión

9.2.1 Deben realizarse revisiones no programadas en respuesta a:

9.2.1.1 Hallazgos relacionados con registros derivados de auditorías internas o externas

9.2.1.2 Incidentes de seguridad en los que los registros fueran inexistentes, estuvieran corruptos o fueran insuficientes

9.2.1.3 Cambios materiales en la infraestructura de TI (p. ej., migración a plataformas de registro en la nube)

9.2.1.4 Actualizaciones de obligaciones regulatorias o legales (p. ej., RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE)

9.3 Control de versiones

9.3.1 Todos los cambios en esta política deben registrarse con número de versión, fecha y resumen de las revisiones

9.3.2 Las versiones anteriores deben archivarse y conservarse durante al menos 3 años

9.3.3 Las políticas actualizadas deben comunicarse a las partes interesadas afectadas, especialmente a aquellas con acceso a nivel de sistema

10. Políticas relacionadas y vinculaciones

10.1 Esta política respalda directamente y está respaldada por las siguientes políticas de seguridad de la información para pymes:

10.1.1 P17S – Política de Protección de Datos y Privacidad: Garantiza que los datos de registro que contienen información personal se gestionen con salvaguardas de integridad, conservación y acceso conformes con los requisitos del RGPD de la UE.

10.1.2 P21S – Política de seguridad de red: Proporciona la base para capturar registros relacionados con cortafuegos, acceso inalámbrico, VPN y supervisión de la segmentación.

10.1.3 P24S – Política de desarrollo seguro: Garantiza que los registros de aplicaciones (p. ej., intentos de inicio de sesión, errores y excepciones) se integren en el diseño y las operaciones del software.

10.1.4 P30S – Política de respuesta a incidentes: Se basa en datos de registro precisos y completos para detectar, analizar y responder a eventos de seguridad de la información.

10.1.5 P23S – Política de sincronización horaria: Garantiza marcas temporales coherentes y trazables en todos los sistemas, permitiendo correlacionar los registros durante las investigaciones.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 8.1 exige la implantación de controles operativos para mitigar los riesgos de seguridad de la información, incluido el registro.

11.2 ISO/IEC 27002

11.2.1 El control 8.15 exige el registro de eventos para respaldar la detección de anomalías y la rendición de cuentas.

11.2.2 El control 8.16 exige la protección de los registros frente a manipulaciones y accesos no autorizados.

11.2.3 El control 8.17 exige la supervisión de los sistemas para detectar actividad inusual y confirmar la eficacia de los controles de supervisión.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 a AU-12 abarcan el contenido del registro de auditoría, su revisión, conservación y alertas automatizadas.

11.3.2 SI-4 exige la detección de anomalías del sistema y la notificación de eventos sospechosos.

11.4 RGPD de la UE

11.4.1 El artículo 5(1)(f) exige la integridad y confidencialidad de los datos personales, lo que incluye el registro del acceso.

11.4.2 El artículo 32 exige medidas técnicas y organizativas para garantizar la seguridad, incluido el registro y la supervisión.

11.4.3 El artículo 33 exige la notificación oportuna de violaciones de seguridad, respaldada por registros que permitan el análisis de causa raíz.

11.5 Directiva NIS2 de la UE

11.5.1 El artículo 21(2)(d) exige mecanismos de registro que detecten anomalías y proporcionen apoyo durante las investigaciones de incidentes.

11.5.2 El artículo 23 exige la notificación de incidentes en un plazo de 24 horas, lo que depende de datos de registro precisos y oportunos.

11.6 DORA de la UE

11.6.1 El artículo 10 exige resiliencia operativa digital, incluida la trazabilidad de los incidentes relacionados con las TIC mediante registro.

11.6.2 El artículo 15 exige la supervisión de proveedores de servicios, incluido el acceso a registros y los derechos de revisión.

11.7 COBIT 2019

11.7.1 DSS01.03 exige la trazabilidad de la actividad del sistema mediante registro y supervisión.

11.7.2 DSS05.02 trata el registro como un control clave en la protección frente al software malicioso y otras actividades no autorizadas.