					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P31S					Título del documento: **Política de recopilación de evidencias y análisis forense**							
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

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1, 6.3, 8	Planificación basada en riesgos, acciones de mejora y controles operativos para la integridad de las evidencias
ISO/IEC 27002:2022	Controles 5.24–5.27	Orientan el manejo seguro, las revisiones posteriores al incidente y las mejoras basadas en evidencias
ISO/IEC 27035-3:2016	Cláusulas 6.3, 6.4, 7	Garantiza la planificación adecuada, la recopilación lícita y el manejo seguro de las evidencias digitales, con documentación de la cadena de custodia
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Preparación forense, protección de registros de auditoría e integración eficaz en la respuesta a incidentes
RGPD de la UE	Artículos 33, 34	Documentación y trazabilidad de brechas de seguridad de los datos personales
Directiva NIS2 de la UE	Artículo 23	Notificación trazable de incidentes y manejo seguro de evidencias
DORA de la UE	Artículo 17(1), 17(2)	Garantiza la recopilación, el almacenamiento y la conservación de evidencias para incidentes relacionados con las TIC, la solidez forense y las consultas regulatorias
COBIT 2019	DSS05.06, DSS05.07	Registro fiable y manejo estructurado de evidencias para investigaciones seguras y auditables

1. Propósito

1.1. Esta política define cómo la organización gestiona las evidencias digitales relacionadas con incidentes de seguridad, brechas de seguridad de los datos o investigaciones internas. Garantiza que las evidencias se recopilen, almacenen y preserven de forma jurídicamente sólida y con la debida preparación para auditorías, dando soporte tanto a la toma de decisiones interna como a posibles actuaciones externas.

1.2. La política permite a las pequeñas organizaciones proteger la integridad de registros, archivos e imágenes de sistemas, al tiempo que demuestra diligencia debida conforme a ISO/IEC 27001, el RGPD de la UE y normas relacionadas.

1.3. Da soporte a la preparación forense sin requerir recursos técnicos avanzados ni un equipo de TI a tiempo completo, mediante la definición de responsabilidades, procesos y requisitos de conservación claros.

2. Alcance

2.1. Esta política aplica a:

2.1.1. Todos los empleados, proveedores de servicios de TI y consultores externos implicados en la respuesta a incidentes, la investigación o el análisis de brechas de seguridad

2.1.2. Todos los sistemas de la empresa, incluidos portátiles, dispositivos móviles, servidores, cuentas de correo electrónico, plataformas SaaS y almacenamiento en la nube (p. ej., Microsoft 365, Google Workspace)

2.1.3. Cualquier evento que requiera evidencias para acciones disciplinarias internas, defensa jurídica, reclamaciones al seguro o interacción con reguladores

2.2. Esto incluye eventos reales y presuntos que impliquen:

2.2.1. Fuga de datos

2.2.2. Amenaza interna o uso indebido

2.2.3. Brechas de seguridad (p. ej., malware, acceso no autorizado)

2.2.4. Quejas de clientes que requieran validación digital

2.2.5. Requerimientos de reguladores o de las fuerzas y cuerpos de seguridad

3. Objetivos

3.1. Garantizar que todas las evidencias se recopilen y gestionen de una manera que preserve su integridad, autenticidad y cadena de custodia.

3.2. Evitar la modificación accidental, eliminación o gestión incorrecta de registros, archivos o imágenes de sistemas que puedan ser necesarios para investigaciones.

3.3. Proporcionar un enfoque coherente y auditable para la gestión de evidencias que cumpla las expectativas legales y regulatorias (p. ej., notificación de brechas conforme al RGPD, trazabilidad conforme a NIS2).

3.4. Definir funciones y responsabilidades claras para garantizar una captura de evidencias rápida, segura y conforme con los requisitos legales durante incidentes de seguridad.

3.5. Dar soporte a la preparación forense en entornos pyme, minimizando la complejidad y evitando interrupciones en las operaciones diarias de la organización.

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Aprueba todas las investigaciones formales que requieran recopilación de evidencias.

4.1.2. Revisa y aprueba formalmente los informes de incidentes que impliquen posibles acciones legales o disciplinarias.

4.1.3. Decide si debe notificarse a asesores jurídicos externos o a reguladores.

4.1.4. Garantiza que la política se revise y actualice periódicamente.

4.2. Proveedor externo de servicios de TI / Administrador de sistemas

4.2.1. Recopila y preserva evidencias digitales siguiendo procedimientos seguros.

4.2.2. Documenta las marcas temporales, los detalles del sistema y las etapas del tratamiento.

4.2.3. Protege todos los materiales recopilados en una ubicación segura.

4.2.4. Presta apoyo al análisis forense 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. Revisión anual de la política

9.1.1. Esta política debe revisarse al menos una vez cada 12 meses por el Director General (DG) para confirmar:

9.1.1.1. El cumplimiento de los controles del Anexo A de ISO/IEC 27001

9.1.1.2. Su vigencia respecto de las plataformas digitales y servicios de TI actuales

9.1.1.3. La adecuación de los procedimientos de registro, conservación de evidencias y preparación forense

9.2. Eventos desencadenantes para la revisión de la política

9.2.1. La política también debe revisarse y actualizarse después de:

9.2.1.1. Cualquier incidente grave que requiera recopilación de evidencias

9.2.1.2. Una auditoría desfavorable o un requerimiento regulatorio en el que se haya cuestionado la integridad de las evidencias

9.2.1.3. La adopción de nuevas herramientas o procedimientos para la respuesta a incidentes o la supervisión del sistema

9.2.1.4. Cambios legales (p. ej., actualizaciones de orientaciones del RGPD o de NIS2)

9.3. Aprobación y distribución de cambios

9.3.1. Todos los cambios deben ser revisados y aprobados por el DG

9.3.2. La versión actualizada debe compartirse con:

9.3.2.1. Los proveedores de TI y consultores que participen en investigaciones

9.3.2.2. Cualquier miembro del personal con responsabilidades de administración de sistemas

9.3.3. Debe conservarse una copia actualizada en el archivo de políticas de la empresa y compartirse con los auditores cuando se solicite

10. Políticas relacionadas e interdependencias

10.1. Esta política es interdependiente con las siguientes políticas alineadas con pymes:

10.1.1. P2S – Política de funciones y responsabilidades de gobernanza: establece la autoridad sobre las investigaciones de incidentes, las decisiones sobre evidencias y el escalado legal/regulatorio.

10.1.2. P4S – Política de control de acceso: garantiza que solo el personal autorizado pueda acceder a sistemas y registros sensibles durante las investigaciones.

10.1.3. P22S – Política de registro y supervisión: proporciona los datos fuente utilizados como evidencias forenses y establece requisitos de conservación, control de acceso y registro.

10.1.4. P30S – Política de respuesta a incidentes: desencadena la necesidad de recopilar evidencias y define el flujo operativo que conduce a la preservación forense.

10.1.5. P17S – Política de protección de datos y privacidad: garantiza que cualquier dato personal recopilado como evidencia se trate lícitamente conforme al RGPD de la UE y a la normativa relacionada.

10.2. Estas políticas funcionan conjuntamente para dar soporte a la defensa jurídica, la integridad de las investigaciones y la preparación para auditorías conforme a ISO/IEC 27001:2022.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. La cláusula 6.1. La planificación basada en riesgos incluye la preparación de la respuesta y los procedimientos de gestión de evidencias.

11.1.2. La cláusula 6.3. Da soporte a las acciones de mejora basadas en evidencias derivadas de incidentes.

11.1.3. La cláusula 8.1. Exige controles operativos para la integridad de las evidencias.

11.2. ISO/IEC 27002

11.2.1. Los controles 5.24–5.27 orientan el manejo seguro, las revisiones posteriores al incidente y las mejoras basadas en evidencias.

11.3. ISO/IEC 27035-3

11.3.1. Las cláusulas 6.3, 6.4 y 7.3 garantizan la planificación adecuada, la recopilación lícita y el manejo seguro de evidencias digitales durante la respuesta a incidentes, incluida la preservación y la documentación de la cadena de custodia.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 y AU-12 garantizan la preparación forense, la protección de registros de auditoría y la integración efectiva de la recopilación de evidencias en el ciclo de vida de la respuesta a incidentes

11.5. NIST SP 800-86

11.5.1. Define las mejores prácticas para adquirir, analizar y proteger evidencias digitales durante la respuesta a incidentes.

11.6. RGPD de la UE

11.6.1. Los artículos 33–34 exigen la documentación y trazabilidad de incidentes y evidencias al notificar brechas de seguridad de los datos personales.

11.7. Directiva NIS2 de la UE (2022/2555)

11.7.1. El artículo 23 exige la notificación trazable de incidentes y el manejo seguro de evidencias para entidades esenciales e importantes.

11.8. DORA de la UE

11.8.1. El artículo 17(1) garantiza que las evidencias relacionadas con incidentes vinculados a las TIC se recopilen y almacenen de un modo que dé soporte a las investigaciones forenses.

11.8.2. El artículo 17(2) exige que las entidades financieras conserven todos los datos y registros pertinentes asociados a eventos de seguridad, en línea con la solidez forense y las consultas regulatorias.

11.9. COBIT 2019

11.9.1. DSS05.06 – Supervisar, detectar y notificar incidentes: enfatiza la necesidad de un registro fiable para apoyar las investigaciones.

11.9.2. DSS05.07 – Investigar y actuar sobre incidentes: exige un manejo estructurado de evidencias para permitir investigaciones seguras y auditables.