					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P31					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	
ISO/IEC 27002:2022	Controles 5.25–5.27, 8	
ISO/IEC 27035:2016	Partes 1 y 3	
NIST SP 800-53 Rev. 5	IR-1 a IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Análisis forense de medios móviles	Análisis forense de dispositivos móviles y medios
NIST SP 800-86	Integración de técnicas forenses	Integración de técnicas forenses en la respuesta a incidentes
RGPD de la UE	Artículo 5, 33–34	
Directiva NIS2 de la UE	Artículo 23(1)–(4)	
DORA de la UE	Artículo 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Finalidad

1.1 Esta política establece un marco estructurado y jurídicamente sólido para la identificación, recopilación, conservación, análisis y eliminación de evidencias digitales durante incidentes de seguridad reales o presuntos.

1.2 Garantiza que los procesos de preparación forense y gestión de evidencias:

1.2.1 Mantengan la integridad probatoria y la cadena de custodia.

1.2.2 Den soporte a investigaciones internas, procedimientos judiciales o notificaciones regulatorias.

1.2.3 Se ajusten a normas forenses aceptadas internacionalmente y a criterios de admisibilidad legal.

1.3 Esta política respalda el compromiso de la organización con una respuesta a incidentes proactiva, el cumplimiento normativo y la transparencia en la gobernanza, minimizando al mismo tiempo la disrupción operativa.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los empleados, contratistas, proveedores y prestadores de servicios que participen en actividades de administración de sistemas, gestión de incidentes o investigación.

2.1.2 Todos los endpoints, servidores, aplicaciones, redes y plataformas en la nube bajo el control de la organización o sujetas a su responsabilidad contractual.

2.1.3 Cualquier incidente o evento que requiera gestión de evidencias, incluidos:

2.1.3.1 amenazas internas, violaciones de la seguridad de los datos o investigaciones por fraude.

2.1.3.2 uso indebido de sistemas o credenciales.

2.1.3.3 incidentes de tecnología operativa (OT) o de control industrial.

2.1.3.4 incumplimientos del control de acceso físico que afecten a activos digitales.

2.2 Esta política también regula cualquier interacción con servicios forenses de terceros o con las fuerzas y cuerpos de seguridad durante escalados legales o procedimientos regulatorios.

3. Objetivos

3.1 Permitir una adquisición de evidencias rápida, segura y conforme a la política durante eventos de seguridad o investigaciones.

3.2 Preservar la integridad, autenticidad y admisibilidad de las evidencias digitales recopiladas mediante un control estricto del acceso, el registro y los procedimientos de verificación.

3.3 Garantizar que todas las actividades forenses se coordinen con las obligaciones legales y regulatorias, incluidas la protección de datos, la legislación laboral y las restricciones a las transferencias internacionales.

3.4 Respaldar el análisis posterior al incidente, la determinación de la causa raíz y la mejora de controles mediante resultados forenses de alta calidad.

3.5 Integrar la preparación forense en el Sistema de Gestión de la Seguridad de la Información (SGSI), dando soporte a auditorías, notificaciones de brechas de seguridad y a la toma de decisiones por parte de la alta dirección.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es responsable de esta política y garantiza que todas las operaciones forenses sean jurídicamente sólidas, auditables y basadas en riesgos.

4.1.2 Autoriza el escalado a entidades legales externas y a proveedores de servicios forenses.

4.2 Analistas forenses / gestores de incidentes

4.2.1 Dirigen la adquisición, conservación y análisis técnico de evidencias.

4.2.2 Garantizan que la cadena de custodia se registre y mantenga correctamente.

4.2.3 Documentan todas las acciones, hallazgos y ajustes de configuración de las herramientas utilizadas durante las investigaciones.

[... 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 al menos una vez al año y actualizarse cuando sea necesario para reflejar:

9.1.1 Cambios en leyes, reglamentos o jurisprudencia que afecten a los procedimientos forenses o a la gestión de datos.

9.1.2 Actualizaciones de normas forenses o conjuntos de herramientas reconocidos por la industria.

9.1.3 Lecciones aprendidas de revisiones posteriores al incidente, litigios o hallazgos de auditoría.

9.1.4 Cambios tecnológicos en plataformas, dispositivos o sistemas objeto de investigación.

9.2 El proceso de revisión es responsabilidad del CISO y debe incluir consulta con:

9.2.1 el área jurídica y de cumplimiento normativo.

9.2.2 el Delegado de Protección de Datos (DPO).

9.2.3 los equipos de operaciones de seguridad y análisis forense.

9.2.4 Auditoría Interna.

9.3 Todas las revisiones deben:

9.3.1 Estar sujetas a control de versiones y almacenarse en el repositorio de políticas.

9.3.2 Comunicarse a las partes interesadas afectadas, incluidos los equipos forenses y de respuesta.

9.3.3 Ir acompañadas de actualizaciones de los procedimientos operativos y materiales de formación pertinentes.

9.4 Deben activarse revisiones extraordinarias tras cualquier incidente crítico que implique una gestión inadecuada de evidencias, un fallo en la cadena de custodia o problemas de admisibilidad legal.

10. Políticas relacionadas y vinculaciones

10.1 Esta política está alineada con las siguientes políticas de la organización y cuenta con su apoyo:

10.1.1 P1 – Política de Seguridad de la Información: establece el mandato fundamental para la investigación, el control de evidencias y el cumplimiento de la legislación aplicable.

10.1.2 P5 – Política de Gestión de Cambios: garantiza que los sistemas bajo investigación no se alteren durante procesos forenses activos.

10.1.3 P14 – Política de Conservación y Eliminación de Datos: regula la eliminación segura y los plazos de conservación de las evidencias y de los datos relacionados con los casos.

10.1.4 P18 – Política de Controles Criptográficos: establece los requisitos de cifrado para almacenar y transferir datos sensibles o con valor probatorio.

10.1.5 P22 – Política de Registro y Supervisión: garantiza la disponibilidad de registros de eventos y telemetría para la recopilación de evidencias y la correlación forense.

10.1.6 P30 – Política de Respuesta a Incidentes: define el triaje de incidentes y las vías de escalado en las que se activan procedimientos forenses.

10.1.7 P33 – Política de Supervisión de Auditoría y Cumplimiento: valida la adhesión a los protocolos forenses y a los requisitos de cadena de custodia mediante auditorías periódicas.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas internacionales de análisis forense y gestión de incidentes, garantizando la integridad de las evidencias, su solidez jurídica y el cumplimiento en distintas jurisdicciones.

11.2 ISO/IEC 27001

11.2.1 Cláusula 8.1 – Da soporte al control operacional de la preparación forense y de los procedimientos de evidencia.

11.3 ISO/IEC 27002

11.3.1 Anexo A, control 5.25 – Responsabilidades para la gestión de incidentes: exige funciones definidas para la gestión de incidentes de seguridad de la información e investigaciones.

11.3.2 Anexo A, control 5.26 – Notificación de eventos de seguridad de la información: respalda la recopilación de artefactos relacionados con eventos como evidencia.

11.3.3 Anexo A, control 5.27 – Respuesta a incidentes de seguridad de la información: exige una remediación e investigación estructuradas y guiadas por la evidencia.

11.3.4 Anexo A, control 8.27 – Desarrollo seguro y análisis forense (cuando proceda): aborda la protección de sistemas y herramientas durante las investigaciones.

11.4 ISO/IEC 27035:2016 (partes 1 y 3)

11.4.1 Establece los principios de detección de incidentes, respuesta y preparación forense, incluida la planificación, la cadena de custodia y la gestión de evidencias de incidentes.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 a IR-9, AU-6, PL-2: define requisitos estructurados para planificar, detectar, analizar, contener y responder a incidentes de seguridad. Respaldan la recopilación y auditabilidad de las evidencias (AU-6) y garantizan la alineación con los planes de seguridad y privacidad del sistema (PL-2) durante las investigaciones forenses.

11.6 NIST SP 800-86

11.6.1 Proporciona directrices para integrar los procesos forenses en el ciclo de vida más amplio de respuesta a incidentes y garantizar la preparación forense.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Se centra en las mejores prácticas para adquirir, conservar y analizar evidencias de medios digitales y dispositivos móviles de forma jurídicamente sólida.

11.8 RGPD de la UE (2016/679)

11.8.1 Artículo 5 – Principios relativos al tratamiento de datos personales: se aplica a evidencias que contengan datos personales o sensibles, garantizando la minimización y la limitación de la finalidad.

11.8.2 Artículos 33–34 – Notificación de violaciones de la seguridad de los datos personales: los datos forenses respaldan el cumplimiento de las obligaciones de notificación de brechas y de los procesos de divulgación legal.

11.9 Directiva NIS2 de la UE (2022/2555)

11.9.1 Artículo 23 – Obligaciones de notificación: la documentación y los hallazgos forenses respaldan informes de incidentes oportunos y precisos a las autoridades competentes.

11.10 DORA de la UE (2022/2554)

11.10.1 Artículo 17 – Notificación de incidentes relacionados con las TIC: exige registros detallados de la causa raíz y de evidencias de incidentes graves relacionados con las TIC, especialmente en el sector financiero.

11.11 COBIT 2019

11.11.1 DSS01.07 – Gestionar los incidentes de seguridad: exige documentación de incidentes y rigor investigador.

11.11.2 DSS05.04 – Gestionar las investigaciones de seguridad: enfatiza la conservación de evidencias digitales y el soporte a acciones disciplinarias y legales.