					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P30					Título del documento: **Política de Respuesta a Incidentes**							
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	Cláusula 8.1, Cláusula 9	Procesos estructurados para la gestión de riesgos y la respuesta a incidentes
ISO/IEC 27002:2022	Controles 5.25–5.27	Funciones, notificación, respuesta y mejora para incidentes
NIST SP 800-53 Rev.5	IR-1 a IR-9	Ciclo de vida integral de respuesta a incidentes
RGPD de la UE	Artículo 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Plazos de notificación de violaciones de seguridad, notificación y comunicación a los interesados
Directiva NIS2 de la UE	Artículo 23(1)–(4)	Notificación a la autoridad nacional y notificación estructurada
DORA de la UE	Artículo 17(1)–(3)	Notificación de incidentes graves relacionados con las TIC para entidades financieras
COBIT 2019	DSS02, DSS04, MEA	Define, supervisa y evalúa la gestión de incidentes, la continuidad y la evaluación

1. Propósito

1.1 Esta política establece una estructura formal para la identificación, notificación, análisis, contención, respuesta, recuperación y revisión posterior al incidente de los incidentes de seguridad de la información que afecten a la organización.

1.2 Garantiza respuestas oportunas, coordinadas y eficaces para minimizar la interrupción operativa, las pérdidas financieras, el daño reputacional y el incumplimiento normativo.

1.3 La política también facilita la mejora continua de la postura de ciberresiliencia de la organización mediante las lecciones aprendidas y la integración de los hallazgos posteriores al incidente en la gobernanza, las herramientas y los programas de formación.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todo el personal, incluidos empleados, contratistas, consultores y proveedores de servicios externos

2.1.2 Todos los sistemas de información, aplicaciones, infraestructuras, redes y datos, ya estén en las instalaciones, en la nube o en entornos híbridos

2.1.3 Todos los tipos de incidentes de seguridad, incluidos, entre otros:

2.1.3.1 Acceso no autorizado o elevación de privilegios

2.1.3.2 Ataques de malware y ransomware

2.1.3.3 Ataques de denegación de servicio (DoS/DDoS)

2.1.3.4 Pérdida, fuga o exfiltración de datos

2.1.3.5 Uso indebido interno o incumplimientos de la política

2.1.3.6 Incidentes de seguridad física que afecten a activos digitales

2.2 La política abarca la detección, el triaje, la investigación, el escalado, la contención, la gestión de evidencias, la notificación, la recuperación y el análisis de causa raíz.

3. Objetivos

3.1 Establecer una capacidad de respuesta a incidentes repetible y escalable que permita la detección, clasificación y mitigación rápidas de los incidentes de seguridad.

3.2 Minimizar el impacto de los eventos de seguridad en las operaciones de la organización mediante procedimientos estructurados de contención, erradicación y recuperación de sistemas.

3.3 Garantizar que la notificación y la respuesta a incidentes se ajusten a los requisitos legales, regulatorios y contractuales, en particular los relativos a los plazos de notificación de violaciones de seguridad y a la gestión de evidencias.

3.4 Reforzar la transparencia y la rendición de cuentas proactiva mediante el registro, la documentación y el seguimiento adecuados de métricas para todos los incidentes de seguridad.

3.5 Promover la mejora continua mediante revisiones posteriores al incidente, acciones correctivas y formación de las partes interesadas.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es responsable del marco de respuesta a incidentes, garantiza la aplicación de la política y supervisa la coordinación de incidentes en toda la organización.

4.1.2 Actúa como enlace principal con los reguladores, la alta dirección y el asesor jurídico externo durante incidentes graves.

4.2 Coordinador de Respuesta a Incidentes

4.2.1 Coordina los equipos de respuesta multifuncionales, gestiona los flujos de trabajo y realiza el seguimiento del estado de la contención y la recuperación.

4.2.2 Activa y dirige la revisión posterior a la implantación (PIR) y garantiza que las acciones correctivas se registren y se implementen.

[... 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 anualmente y actualizarse cuando sea necesario para incorporar:

9.1.1 Cambios en el panorama de amenazas, los tipos de incidentes o los vectores de ataque

9.1.2 Lecciones aprendidas de incidentes graves, cuasiincidentes o hallazgos regulatorios

9.1.3 Actualizaciones de leyes y reglamentos aplicables (p. ej., RGPD de la UE, DORA de la UE, Directiva NIS2 de la UE)

9.1.4 Retroalimentación de los usuarios procedente de simulacros de respuesta a incidentes y revisiones posteriores al incidente

9.2 El Director de Seguridad de la Información es responsable de iniciar y coordinar el proceso de revisión, en consulta con:

9.2.1.1 Asesoría Jurídica y DPD

9.2.1.2 SOC y Operaciones de TI

9.2.1.3 Equipos de continuidad del negocio y gestión de riesgos

9.2.1.4 Alta dirección

9.3 Los cambios en la política deben:

9.3.1 Documentarse en un repositorio sujeto a control de versiones

9.3.2 Comunicarse a todos los equipos afectados y reflejarse en la formación de concienciación

9.3.3 Validarse mediante ejercicios de mesa o ejercicios en vivo de respuesta a incidentes dentro de los tres meses siguientes a su aprobación

9.4 Las actualizaciones urgentes motivadas por amenazas emergentes, hallazgos de auditoría o nuevas obligaciones legales deben aplicarse de inmediato y reflejarse en el historial de revisiones de la política.

10. Políticas relacionadas y vinculaciones

10.1 Esta política está respaldada por las siguientes políticas de la organización y depende de ellas:

10.1.1 P1 – Política de Seguridad de la Información: Establece el requisito general de operaciones basadas en riesgos y preparadas para incidentes.

10.1.2 P5 – Política de Gestión de Cambios: Garantiza que las actividades de contención y recuperación que afecten a infraestructuras o servicios sigan procedimientos formales.

10.1.3 P13 – Política de Clasificación y Etiquetado de Datos: Respalda la clasificación de la severidad de los incidentes en función de la sensibilidad de los datos.

10.1.4 P15 – Política de Copias de Seguridad y Restauración: Permite la recuperación frente a ransomware o ataques destructivos con garantía de integridad.

10.1.5 P18 – Política de Controles Criptográficos: Define medidas de cifrado que reducen el impacto de los incidentes y los riesgos de exposición de datos.

10.1.6 P22 – Política de Registro y Supervisión: Proporciona la visibilidad de eventos, las alertas y la conservación de registros fundamentales para una detección eficaz y el análisis forense.

10.1.7 P29 – Política de Datos de Prueba y Entornos de Prueba: Garantiza que los incidentes que afecten a sistemas no productivos también se gestionen de manera estructurada y segura.

10.1.8 P33 – Política de Supervisión de Auditoría y Cumplimiento: Valida la preparación ante incidentes y la eficacia de la respuesta mediante auditorías estructuradas y evaluaciones de cumplimiento.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001: Cláusula 8.1 – Planificación y control operacional: Procesos estructurados para gestionar riesgos y planificar la respuesta a incidentes.

11.2 ISO/IEC 27002:2022 – Controles 5.25–5.27: Responsabilidades para la gestión de incidentes, notificación, respuesta, comunicación y mejora.

11.3 NIST SP 800-53 Rev.5: IR-1 a IR-9, AU-6, PL-2: Requisitos integrales para el ciclo de vida de respuesta a incidentes, auditoría y planificación de la seguridad.

11.4 RGPD de la UE: Artículos 33/34: Obligaciones de notificación a las autoridades de control y requisitos de comunicación a los interesados (con excepciones definidas).

11.5 Directiva NIS2 de la UE (2022/2555): Artículo 23: Notificación nacional obligatoria, con obligaciones de notificación intermedia y final.

11.6 DORA de la UE (2022/2554): Artículo 17: Requisitos de notificación a las autoridades de incidentes relacionados con las TIC en entidades financieras.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Gestión de incidentes del servicio y continuidad, además de supervisión del rendimiento y la conformidad.