					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P39					Título del documento: **Política de divulgación coordinada de vulnerabilidades**							
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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev. 5	RA-5, SI-2, PM-15, CA-8, SR-6	
RGPD de la UE	Art. 32(1)(d)	
Directiva NIS2 de la UE	Art. 21(2)(e)	
DORA de la UE	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Propósito

1.1 Establecer un proceso formal para la recepción, gestión y divulgación de información sobre vulnerabilidades que afecten a los sistemas o servicios de la organización, en cumplimiento de lo exigido por el artículo 21(2)(e) de la Directiva NIS2 de la UE en materia de gestión y divulgación de vulnerabilidades.

1.2 Fomentar que investigadores de seguridad externos, socios y usuarios notifiquen vulnerabilidades de forma responsable (divulgación coordinada de vulnerabilidades, CVD) y definir la forma en que la organización comunica la información sobre vulnerabilidades a las partes interesadas.

2. Alcance

2.1 Esta política se aplica a todos los sistemas de red y de información propiedad de la organización u operados por esta, así como a cualquier vulnerabilidad identificada en dichos sistemas.

2.2 Abarca a los equipos internos de seguridad, TI y desarrollo, así como a cualquier tercero que notifique vulnerabilidades (por ejemplo, investigadores, clientes o proveedores). También regula las comunicaciones con proveedores de productos o servicios cuando sus componentes estén implicados en la vulnerabilidad.

3. Objetivos

3.1 Detectar y subsanar vulnerabilidades de seguridad de manera oportuna, aprovechando tanto las evaluaciones internas como las divulgaciones externas.

3.2 Proporcionar directrices claras para que los notificantes externos remitan información sobre vulnerabilidades de forma segura y lícita, y para que la organización responda y remedie eficazmente.

3.3 Garantizar la alineación con los requisitos de la Directiva NIS2 de la UE y con las mejores prácticas del sector (ISO/IEC 29147 e ISO/IEC 30111) para la divulgación coordinada de vulnerabilidades, mejorando la seguridad global del ecosistema.

4. Funciones y responsabilidades

4.1 Equipo de Respuesta a Vulnerabilidades (VRT): equipo designado, dirigido por el Director de Seguridad de la Información o por el responsable de gestión de vulnerabilidades, que recibe y realiza el triaje de las notificaciones de vulnerabilidades, evalúa el riesgo y el impacto, y coordina la remediación y la divulgación pública.

4.2 Equipos de TI y desarrollo: colaboran con el VRT para validar las vulnerabilidades notificadas, desarrollar y probar parches o medidas de mitigación, y desplegar correcciones. También aportan detalles técnicos para los avisos 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. Supervisión y auditoría

9.1 El VRT mantendrá un registro de divulgación de vulnerabilidades para el seguimiento de cada notificación desde su recepción hasta su cierre. Este registro se revisará mensualmente para garantizar el avance oportuno de los elementos abiertos. Los elementos vencidos se escalarán.

9.2 La auditoría interna o un evaluador de seguridad independiente revisará anualmente la eficacia del proceso de gestión de vulnerabilidades; por ejemplo, comprobando que muestras de casos de vulnerabilidades se hayan tratado conforme a la política (acuse de recibo, corrección y divulgación en plazo). También verificará que el canal público de divulgación orientado al exterior funcione correctamente (por ejemplo, que los correos de prueba se reciban y se gestionen).

9.3 Las métricas sobre vulnerabilidades (volumen por severidad, tiempos de remediación, etc.) se recopilarán trimestralmente y se presentarán al comité de gobierno de ciberseguridad para respaldar las actualizaciones de la evaluación de riesgos.

10. Revisión y mantenimiento

10.1 Esta política se revisará al menos una vez al año. Además, cualquier cambio significativo en nuestro entorno de TI (por ejemplo, el lanzamiento de un nuevo servicio expuesto a Internet) o la evolución normativa aplicable (por ejemplo, nueva legislación de la UE sobre divulgación de vulnerabilidades de productos) desencadenará una revisión extraordinaria.

10.2 Las actualizaciones de la política incorporarán la retroalimentación de los notificantes externos y las lecciones extraídas de los análisis internos posteriores a incidentes. Los cambios relevantes serán aprobados por el Director de Seguridad de la Información, comunicados a todos los empleados y publicados en nuestro repositorio en línea de políticas de seguridad para garantizar la transparencia.

11. Políticas relacionadas y vinculaciones

11.1 P01 – Política de Seguridad de la Información. Mandato de gestión para la gestión y divulgación de vulnerabilidades.

11.2 P19 – Política de gestión de vulnerabilidades y parches. Proceso interno de remediación vinculado a la recepción de CVD.

11.3 P24 – Política de Desarrollo Seguro. Aporta correcciones y refuerzo del SDLC a partir de las incidencias notificadas.

11.4 P25 – Política de requisitos de seguridad de las aplicaciones. Garantiza que los productos dispongan de requisitos de seguridad preparados para la divulgación.

11.5 P30 – Política de Respuesta a Incidentes. Gestiona la explotación activa de vulnerabilidades divulgadas.

11.6 P31 – Política de recopilación de evidencias y análisis forense. Conserva los artefactos derivados de deficiencias notificadas o explotadas.

11.7 P26 – Política de Seguridad de Terceros y Proveedores. Coordina divulgaciones que afecten a componentes de proveedores.

11.8 P37 – Política de Cumplimiento Jurídico y Normativo. Regula la notificación, la redacción de la salvaguarda de buena fe y la publicación.

12. Referencias

12.1 Directiva NIS2 (UE 2022/2555), artículo 21(2), letra (e) (seguridad en el desarrollo y gestión y divulgación de vulnerabilidades)

12.2 Reglamento de Ejecución (UE) 2024/2690 de la Comisión, anexo, sección 6.10 (requisitos técnicos sobre procesos de gestión y divulgación de vulnerabilidades)

12.3 Guía técnica de ENISA sobre medidas de gestión del riesgo de ciberseguridad – sección sobre gestión y divulgación de vulnerabilidades

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (control A.5.7 sobre inteligencia de amenazas y divulgación de vulnerabilidades; control A.8.28 sobre desarrollo seguro)

12.5 ISO/IEC 29147:2018 (directrices para la divulgación de vulnerabilidades) e ISO/IEC 30111:2019 (directrices para procesos de gestión de vulnerabilidades)