					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P19					Título del documento: **Política de gestión de vulnerabilidades y parches**							
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**

Aviso legal (derechos de autor y restricciones de uso)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: info@clarysec.com

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Tratamiento sistemático de las vulnerabilidades técnicas; eficacia continua de los controles de seguridad.
ISO/IEC 27002:2022	Controles 8.8, 8.9, 5	Guía de implantación para la aplicación de parches, el escaneo de vulnerabilidades, la integridad del software, la configuración segura y los inventarios de activos.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Se exigen escaneos frecuentes, remediación de fallos y gestión de la configuración.
RGPD de la UE	Artículo 32, Considerando 49	Medidas técnicas para la aplicación de parches sin demora, la gestión de vulnerabilidades y la continuidad de la seguridad.
Directiva NIS2 de la UE	Artículo 21(2)(d)	Detección, respuesta y mitigación de vulnerabilidades para mantener un alto nivel de ciberhigiene.
DORA de la UE	Artículos 8, 10(2)(f)	Remediación oportuna de vulnerabilidades de las TIC; evaluaciones continuas guiadas por amenazas.
COBIT 2019	DSS05.02, DSS01.03, MEA	Identificar, supervisar y mitigar debilidades técnicas; supervisar indicios de explotación; auditar la eficacia, incluido el estado de los parches.

1. Finalidad

1.1 Esta política define los requisitos obligatorios de la organización para identificar, clasificar, remediar y supervisar las vulnerabilidades técnicas y los fallos de software en todos los sistemas y activos de información dentro del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI).

1.2 Garantiza que todas las vulnerabilidades conocidas se evalúen y traten de manera oportuna y basada en el riesgo, mediante la aplicación coordinada de parches, ajustes de configuración o controles compensatorios, en consonancia con las necesidades de la organización y las obligaciones de cumplimiento.

1.3 Esta política respalda el cumplimiento del control 8.8 del Anexo A de ISO/IEC 27001 y de la guía ISO/IEC 27002, y atiende requisitos regulatorios conforme al artículo 8 de DORA, el artículo 21 de NIS2, el artículo 32 del RGPD de la UE y los dominios DSS y APO de COBIT 2019.

2. Alcance

2.1 Esta política se aplica a todos los sistemas de información, activos y entornos que almacenan, procesan o transmiten datos sujetos al gobierno del SGSI, incluidos:

2.1.1 Sistemas operativos, aplicaciones, dispositivos de red, firmware, plataformas en la nube, interfaces de programación de aplicaciones y software de terceros.

2.1.2 Sistemas en entornos de desarrollo, preproducción, producción, copia de seguridad y recuperación ante desastres.

2.1.3 Endpoints, servidores, dispositivos IoT, infraestructura de virtualización y contenedores.

2.2 Es de obligado cumplimiento para:

2.2.1 Personal interno: administradores de TI, ingenieros de sistemas, desarrolladores de aplicaciones, analistas de seguridad y equipos de infraestructura.

2.2.2 Partes externas: contratistas, proveedores de servicios gestionados (MSP), proveedores de software e integradores de sistemas con responsabilidades técnicas sobre activos incluidos en el alcance.

2.3 La política abarca el ciclo de vida completo de la gestión de vulnerabilidades y parches, incluyendo:

2.3.1 Escaneo y detección.

2.3.2 Clasificación y priorización del riesgo.

2.3.3 Obtención, pruebas, despliegue y reversión de parches.

2.3.4 Gestión de excepciones y planificación de controles compensatorios.

2.3.5 Registro de eventos, elaboración de informes y trazabilidad de auditoría.

3. Objetivos

3.1 Garantizar que todas las vulnerabilidades conocidas se identifiquen, evalúen y remedien de forma que se minimice la exposición al riesgo y se mantenga la alineación con las prioridades operativas.

3.2 Establecer procesos homogéneos en toda la organización para el escaneo de vulnerabilidades, la clasificación de severidad (por ejemplo, CVSS) y la gestión de parches, incluida la gestión de emergencias y la planificación de la reversión.

3.3 Habilitar una gestión segura de la configuración mediante la alineación con configuraciones de referencia, controles de endurecimiento, prácticas de gestión de cambios e inteligencia de amenazas en tiempo real.

3.4 Proporcionar un cumplimiento medible de controles regulatorios y normativos relacionados con la integridad de los sistemas, la higiene de parches y la remediación oportuna de fallos.

3.5 Definir la responsabilidad proactiva y la rendición de cuentas entre funciones para todo el ciclo de vida de la gestión de vulnerabilidades, garantizando que todas las partes interesadas actúen dentro de los acuerdos de nivel de servicio definidos y reporten métricas de control sujetas a notificación.

3.6 Favorecer la preparación para auditorías y mejorar la resiliencia frente a amenazas emergentes, incluidas vulnerabilidades de día cero, cadenas de explotación activas y divulgaciones relevantes de proveedores.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de la política y garantiza su integración en el SGSI.

4.1.2 Define la postura de riesgo de la organización y garantiza la alineación con las expectativas regulatorias y de control.

4.2 Responsable de gestión de vulnerabilidades / Responsable de operaciones de seguridad

4.2.1 Supervisa de extremo a extremo las operaciones de gestión de vulnerabilidades y parches.

4.2.2 Coordina los calendarios de escaneo, los modelos de priorización y los plazos de remediación.

4.2.3 Mantiene el Registro de Vulnerabilidades y colabora en la evaluación de controles compensatorios.

[... 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 o cuando se produzca cualquiera de las siguientes circunstancias:

9.1.1 Actualizaciones regulatorias significativas (por ejemplo, cambios en DORA o NIS2).

9.1.2 Cambios en los marcos de priorización de vulnerabilidades (por ejemplo, actualizaciones de CVSS).

9.1.3 Cambios importantes en el entorno de TI (por ejemplo, migración a la nube o renovación significativa del EDR).

9.1.4 Incidentes de seguridad de especial relevancia o avisos externos que requieran el refuerzo de la política.

9.2 Las revisiones serán realizadas por el CISO en colaboración con Operaciones de Seguridad, Gestión de Riesgos y la dirección de Infraestructura.

9.3 Las actualizaciones de la política deben:

9.3.1 Documentarse en el registro documental del SGSI.

9.3.2 Ser revisadas y aprobadas por la alta dirección.

9.3.3 Comunicarse a todas las partes interesadas afectadas, incluidos los encargados del tratamiento externos.

9.4 Las versiones históricas se conservarán de forma segura a efectos de auditoría y trazabilidad de responsabilidades.

10. Políticas relacionadas y vinculaciones

10.1 P01 Política de seguridad de la información. Establece el compromiso general de proteger sistemas y datos, lo que incluye la gestión proactiva de vulnerabilidades y la garantía de la integridad del software.

10.2 P05 Política de gestión de cambios. Regula todo despliegue de parches y ajuste de configuración, exigiendo documentación, pruebas, aprobación y procedimientos de reversión que complementan los procesos de remediación de vulnerabilidades.

10.3 P6 - Política de gestión de riesgos. Respalda la clasificación y el tratamiento de vulnerabilidades no remediadas mediante evaluaciones de riesgos estructuradas, análisis de impacto y procedimientos de aceptación del riesgo residual.

10.4 P12 - Política de gestión de activos. Garantiza que los sistemas estén inventariados y clasificados con precisión, permitiendo un escaneo de vulnerabilidades coherente, la asignación de titularidad y la cobertura de parches a lo largo del ciclo de vida.

10.5 P22 - Política de registro de eventos y supervisión. Define requisitos para la detección de eventos y la generación de trazas de auditoría. Esta política proporciona visibilidad sobre la actividad de parcheado, los cambios no autorizados y los intentos de explotación dirigidos a vulnerabilidades conocidas.

10.6 P30 - Política de respuesta a incidentes. Especifica protocolos de escalado y estrategias de contención para vulnerabilidades explotadas, investigaciones de brechas de seguridad y acciones correctivas alineadas con los controles de esta política.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001: cláusula 8.1 - Planificación y control operacional: exige el tratamiento sistemático de las vulnerabilidades técnicas para garantizar la eficacia continua de los controles de seguridad.

11.2 ISO/IEC 27002:2022 - controles 8.8, 8.9, 5: proporciona guía de implantación para la aplicación de parches, el escaneo de vulnerabilidades, la integridad del software y la integración con la configuración segura y los inventarios de activos.

11.3 NIST SP 800-53 Rev.5: RA-5 - supervisión y escaneo de vulnerabilidades: exige escaneos frecuentes y seguimiento de la remediación. SI-2 - remediación de fallos: exige la evaluación y mitigación sin demora de fallos mediante parches disponibles u otras acciones. CM-2 / CM-6 - configuraciones de referencia y controles de gestión de la configuración: establece la base para configuraciones seguras del sistema vinculadas a la aplicación de parches.

11.4 RGPD de la UE (2016/679): artículo 32 - seguridad del tratamiento: exige la implantación de medidas técnicas apropiadas, como la aplicación de parches sin demora y la gestión de vulnerabilidades, para garantizar la confidencialidad y la resiliencia de los sistemas. Considerando 49: anima a las entidades a implantar controles preventivos frente a amenazas conocidas para respaldar la seguridad y la continuidad.

11.5 Directiva NIS2 de la UE (2022/2555): artículo 21(2)(d): obliga a las entidades esenciales e importantes a detectar, responder y mitigar vulnerabilidades de los sistemas y a mantener un alto nivel de ciberhigiene.

11.6 DORA de la UE (2022/2554): artículo 8 - Gestión del riesgo de las TIC: exige la identificación y remediación oportuna de vulnerabilidades en las tecnologías de la información y las comunicaciones utilizadas en sistemas financieros. Artículo 10(2)(f): enfatiza las evaluaciones continuas de vulnerabilidades guiadas por amenazas y la aplicación de parches como parte de la resiliencia operativa.

11.7 COBIT 2019: DSS05.02 - Gestionar las vulnerabilidades de seguridad: orienta a las organizaciones a identificar, supervisar y mitigar debilidades técnicas conocidas. DSS01.03 - supervisar la infraestructura: garantiza que los sistemas se supervisen en busca de indicios de explotación o debilidad. MEA03 - supervisar, evaluar y valorar el cumplimiento: exige la auditoría periódica de la eficacia de los controles, incluido el estado de los parches y la gestión de excepciones.