					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P19S					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	
ISO/IEC 27002:2022	Controles 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Directiva NIS2 de la UE	Artículos 21(2)(d), 21(2)(e)	
DORA de la UE	Artículos 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
RGPD de la UE	Artículo 32(1)(b)	

1. Propósito

1.1 Esta política establece cómo la organización identifica, evalúa y mitiga vulnerabilidades en sistemas, aplicaciones e infraestructura.

1.2 Su finalidad es reducir el riesgo de ciberseguridad mediante la aplicación oportuna de parches y prácticas de remediación basadas en el riesgo adecuadas para pequeñas y medianas empresas (pymes).

1.3 Esta política respalda el cumplimiento de ISO/IEC 27001:2022 y contribuye a satisfacer las obligaciones regulatorias en virtud del RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE, al exigir la gestión proactiva de vulnerabilidades técnicas.

1.4 La organización reconoce que los sistemas sin parchear representan una amenaza significativa para la seguridad de la información y deben gestionarse de forma sistemática y sin demora.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los servidores, equipos de sobremesa, portátiles, dispositivos móviles, equipos de red y plataformas alojadas en la nube utilizados por la organización.

2.1.2 Todos los sistemas operativos, programas de terceros, complementos y aplicaciones utilizados en las operaciones de la organización.

2.1.3 Todo el personal interno de TI y los proveedores de servicios externos responsables del mantenimiento, la actualización o la supervisión de sistemas.

2.1.4 Todo el código desarrollado a medida o software embebido mantenido por la organización o en su nombre.

2.2 La política abarca tanto la infraestructura gestionada directamente por la organización como los sistemas administrados por proveedores externos o proveedores de alojamiento.

3. Objetivos

3.1 Identificar y evaluar de forma oportuna y coherente las vulnerabilidades conocidas en todos los activos de TI.

3.2 Aplicar parches y actualizaciones de software en función de la severidad y del riesgo para las operaciones de la organización o para los datos personales.

3.3 Prevenir la explotación de debilidades técnicas que puedan dar lugar a interrupciones del servicio, brechas de seguridad de los datos o incumplimientos legales.

3.4 Mantener registros precisos de los parches aplicados, las incidencias pendientes y las excepciones, a fin de garantizar la preparación para auditorías.

3.5 Utilizar herramientas y procesos adecuados al tamaño de la organización y a su complejidad operativa, sin comprometer la eficacia.

3.6 Respaldar el cumplimiento legal y normativo, incluido el artículo 32 del RGPD de la UE y el control 8 del anexo A de ISO/IEC 27001.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Asume la responsabilidad general de garantizar la ejecución de las actividades de gestión de vulnerabilidades y parches.

4.1.2 Aprueba las excepciones de riesgo cuando no sea posible aplicar parches y revisa las estrategias de mitigación correspondientes.

4.1.3 Revisa los informes sobre el estado de aplicación de parches y garantiza la disponibilidad de recursos para cumplir las obligaciones establecidas.

4.2 Proveedor de soporte de TI / Responsable interno de TI

4.2.1 Supervisa los sistemas para detectar vulnerabilidades y parches disponibles mediante alertas de proveedores, avisos de amenazas y notificaciones del sistema operativo.

4.2.2 Aplica actualizaciones del sistema operativo, firmware y aplicaciones dentro de los plazos definidos.

4.2.3 Mantiene un registro formal de parches y documenta las actualizaciones pendientes o aplazadas.

4.2.4 Realiza pruebas y planifica las actualizaciones críticas para minimizar las interrupciones operativas.

[... 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

9.1.1 Esta política debe revisarse al menos una vez al año por el Director General, con aportaciones del proveedor de TI y del Responsable de Privacidad.

9.2 Desencadenantes de revisión

9.2.1 Deben realizarse revisiones intermedias si:

9.2.1.1 Una vulnerabilidad grave o un exploit significativo afecta a los sistemas incluidos en el alcance.

9.2.1.2 Se producen cambios significativos en sistemas o software.

9.2.1.3 Una auditoría identifica deficiencias en los procesos de gestión de parches.

9.2.1.4 Se registra un incidente o una brecha de seguridad relacionada con la gestión de parches.

9.3 Control de versiones de la política

9.3.1 Todas las actualizaciones deben registrarse en el control de versiones con un resumen de los cambios.

9.3.2 Los cambios deben comunicarse al personal afectado.

9.3.3 Las versiones obsoletas deben archivarse con acceso restringido.

10. Políticas relacionadas y vínculos

10.1 Esta política respalda y depende de varias políticas para pymes:

10.1.1 P12S – Política de Gestión de Activos: identifica la titularidad y la clasificación de los sistemas, garantizando que todos los activos que requieren parches estén registrados e inventariados.

10.1.2 P14S – Política de Conservación y Eliminación de Datos: garantiza que los sistemas programados para su retirada se actualicen de forma segura o se sometan a borrado seguro, reduciendo la exposición a vulnerabilidades.

10.1.3 P17S – Política de Protección de Datos y Privacidad: prioriza la remediación de vulnerabilidades en los sistemas que tratan datos personales para cumplir la normativa de privacidad.

10.1.4 P22S – Política de Registro de Eventos y Supervisión: respalda la detección de sistemas sin parchear o de comportamientos sospechosos que puedan indicar la explotación de una vulnerabilidad.

10.1.5 P30S – Política de Respuesta a Incidentes: define los procedimientos para responder a vulnerabilidades que den lugar a incidentes de seguridad, incluidos los pasos de escalado y notificación.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 8.1 exige la implantación de controles para abordar el riesgo operativo, incluida la gestión de vulnerabilidades.

11.2 ISO/IEC 27002

11.2.1 El control 8.8 especifica procesos para detectar y corregir debilidades conocidas en los sistemas.

11.2.2 El control 8.9 hace hincapié en la configuración segura, la validación de parches y el control de cambios para evitar nuevas exposiciones durante las actualizaciones.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 exige la identificación de vulnerabilidades y su remediación dentro de plazos definidos.

11.3.2 SI-2 exige la aplicación inmediata de parches y actualizaciones en función de la severidad.

11.3.3 CM-2 regula las configuraciones de referencia del sistema y la documentación de actualizaciones para garantizar protecciones coherentes.

11.4 RGPD de la UE

11.4.1 El artículo 32(1)(b) exige que las organizaciones implanten medidas técnicas adecuadas, incluida la aplicación de parches, para mantener la seguridad del tratamiento.

11.5 Directiva NIS2 de la UE

11.5.1 El artículo 21(2)(d) exige la gestión de vulnerabilidades mediante detección sistemática y remediación.

11.5.2 El artículo 21(2)(e) exige la configuración segura y la gestión de parches para garantizar la resiliencia de las TIC.

11.6 DORA de la UE

11.6.1 El artículo 8(1) exige la detección y mitigación de los riesgos de las TIC, incluidas las vulnerabilidades técnicas.

11.6.2 El artículo 10(2) exige a las entidades financieras remediar debilidades que afecten a los sistemas y operaciones de TIC.

11.7 COBIT 2019

11.7.1 DSS05.02 exige el tratamiento de vulnerabilidades técnicas conocidas para mantener operaciones seguras.

11.7.2 APO12.01 alinea la gestión de riesgos con la supervisión proactiva y la corrección de debilidades del sistema.