Política Específica de Gestión de Vulnerabilidades Técnicas

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

Esta política tiene como objetivo establecer un marco para la identificación, evaluación, mitigación y monitoreo de vulnerabilidades técnicas en los sistemas, aplicaciones y servicios de la organización, asegurando la protección de la información y la continuidad del negocio en conformidad con el control 8.8 de la norma ISO/IEC 27001:2022.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, clausula 8.8.

3. RESPONSABILIDADES

Oficial de seguridad de la información (OSI): Supervisar la aplicación de esta política y la gestión de vulnerabilidades. Revisar y aprobar las clasificaciones de riesgo y los plazos de mitigación.
Equipo de TI y Desarrollo: Implementar controles de seguridad, realizar análisis de vulnerabilidades y aplicar medidas correctivas.
Usuarios y Proveedores: Cumplir con los procedimientos de gestión de vulnerabilidades establecidos en esta política.

Rol/Área/Responsabilidad

Gerencia de TI / Nube Garantizar los recursos de hardware/software (ej. software de escaneo, Wazuh) y asignar tiempo para las tareas de parcheo y mitigación.
Equipo de Desarrollo de Software Garantizar que el código desarrollado internamente esté libre de vulnerabilidades conocidas y que las librerías de terceros se mantengan actualizadas.
Oficial de seguridad (OSI).
Equipo de Operaciones Ejecutar los escaneos de vulnerabilidades, realizar las pruebas de parches y documentar el cierre de la vulnerabilidad.

4. POLÍTICA ESPECÍFICA

Esta Política determina gestionar los accesos a la información. Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad.

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Todo trabajador de DACTA o tercero para el desempeño de sus funciones, se compromete a lo siguiente:

POLÍTICA DE GESTIÓN DE VULNERABILIDADES TÉCNICAS

1. Objetivo
2. Alcance

Esta política aplica a todos los sistemas, infraestructuras, aplicaciones, redes y servicios en la nube de la organización, así como al personal interno y proveedores que intervengan en su desarrollo, operación y mantenimiento.

4. Identificación y Evaluación de Vulnerabilidades

Se realizarán escaneos de vulnerabilidades periódicos en sistemas, aplicaciones y redes con herramientas especializadas como Nessus, OpenVAS, Qualys, Burp Suite, entre otras.

Se integrarán análisis de seguridad en el ciclo de desarrollo de software (DevSecOps) mediante pruebas SAST, DAST y SCA.

Las vulnerabilidades detectadas serán evaluadas utilizando el Common Vulnerability Scoring System (CVSS) para determinar su criticidad y priorización.

5. Mitigación y Corrección

Se aplicarán los parches y actualizaciones de seguridad de manera pertinente.

Vulnerabilidades Medias/Bajas: según cronograma definido por el equipo de seguridad.

Si una vulnerabilidad no puede corregirse de inmediato, se deberá implementar una medida de mitigación temporal y documentar la justificación.

6. Monitoreo y Control

Se establecerá un monitoreo continuo de eventos de seguridad mediante herramientas SIEM (ejemplo: Splunk, Wazuh, ELK Stack).

Se realizarán pruebas de penetración periódicas y auditorías de seguridad para validar la eficacia de las medidas implementadas.

Se llevará un registro documentado de las vulnerabilidades detectadas, las acciones correctivas tomadas y su estado de resolución.

7. Cumplimiento y Auditoría

Esta política será revisada y actualizada anualmente o cuando sea necesario ante cambios tecnológicos o regulatorios.

El cumplimiento de esta política será evaluado mediante auditorías internas y externas alineadas con ISO/IEC 27001:2022.

8. Sanciones por Incumplimiento

El incumplimiento de esta política podrá derivar en sanciones disciplinarias según el reglamento interno de la organización, incluyendo la suspensión del acceso a sistemas o la terminación del contrato en casos graves.

5. AUDITORÍA

- El Oficial de Seguridad de la Información de DACTA se encargará de realizar la revisión de este control trimestralmente.
- Específicamente se revisará el registro con los privilegios de accesos a los datos personales.

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	22/10/2025	Emisión	OSI	Comité SIG	Gerente General
2					
Firmas de la versión vigente			 S. Rafaile	 S. Rafaile	
			 A. Morales	 A. Morales	G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	