intiza

Gestión de Vulnerabilidades y Parches

Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO **Consultoría Externa**	 **Carla Leiva - CISO**	 **Francisco Canale - Director**

NORMA DE GESTIÓN DE VULNERABILIDADES Y PARCHES	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 09/08/2024
Código: NO-SI-13- Gestión de Vulnerabilidades y Parches	Versión: 2.1

Contenido

1. Objetivo

Establecer los lineamientos generales correspondientes a la gestión de vulnerabilidades de INTIZA con el fin de prevenir de manera proactiva la explotación de vulnerabilidades y la pérdida potencial de datos sensibles de la organización.

Por otro lado, se deberá identificar, detectar, clasificar y priorizar adecuadamente las vulnerabilidades con el objetivo de monitorear su respectiva remediación y mitigación.

2. Alcance

Esta norma involucra a todas las personas que realicen cualquier actividad para INTIZA, como los empleados efectivos, personal pasante, contratado, tercerizados o cualquier otra modalidad de empleo directa o indirectamente que pudiera generar un vínculo laboral.

La norma de gestión de vulnerabilidades abarca todos los recursos tecnológicos y sistemas que son propiedad, operados, mantenidos y controlados por INTIZA.

3. Responsabilidades

Seguridad de la Información será quien realice o delegue la gestión de vulnerabilidades en algún responsable de su área.

4. Consideraciones Generales

Definimos como recursos internos a todos aquellos sistemas que son propiedad, operados, mantenidos y controlados por INTIZA e incluyen todos los dispositivos de red (firewalls, routers, switches, etc), servidores (servidores virtuales junto con su correspondiente sistema

operativo y aplicaciones que residen en ellos) y cualquier otro recurso del sistema que se considere dentro del alcance.

Definimos como recursos externos a todos aquellos sistemas que son propiedad, operados, mantenidos y controlados por cualquier entidad que no sea INTIZA, pero para los cuales estos mismos recursos pueden afectar la confidencialidad, integridad y disponibilidad y la seguridad general de los recursos internos de la organización

5. Desarrollo

5.1. Administración de Parches y Actualizaciones

El responsable de Seguridad de la Información será responsable de administrar, gestionar y asegurar, la necesidad de la aplicación de nuevos parches de seguridad (software) aprobados y homologados por la organización.

Todo el software instalado se mantendrá de manera oportuna en los niveles establecidos en los estándares de seguridad, con parches y actualizaciones apropiadas, para abordar las vulnerabilidades y reducir o prevenir cualquier impacto negativo en las operaciones de INTIZA.

5.2. Análisis de Escaneos de Vulnerabilidades

- Se deben realizar escaneos de Vulnerabilidades de los aplicativos críticos de INTIZA con una periodicidad semestral, o cuando haya algún cambio significativo que así lo amerite o el negocio lo requiera.
- Se debe realizar el análisis preliminar del escaneo de vulnerabilidades a ejecutarse. Es responsabilidad de seguridad de la información el relevamiento con las diferentes áreas, identificando los activos estratégicos y críticos para la empresa; una vez identificados los mismos se debe establecer el alcance del análisis definiendo

claramente los equipos, el tipo de software y servicios que prestan, equipos que interactúan y redes donde se encuentran que serán analizados

Para que sea exitoso un análisis de vulnerabilidad, se definen los siguientes lineamientos básicos:

5.2.1. Configuración Inicial

- Solicitar permisos para ejecutar el análisis: Este punto se realiza mediante una solicitud de gestión de cambios con toda la información solicitada.
- Actualizar las herramientas: Las herramientas se actualizan a sus versiones más actuales para una detección óptima.
- Configurar las herramientas: Se realiza la configuración de las herramientas de gestión de Vulnerabilidades utilizadas y/o homologadas por INTIZA.

5.2.2. Análisis de Vulnerabilidades

- Identificar y categorizar las vulnerabilidades potenciales en cada uno de los recursos.
- Identificar falsos positivos corroborando con otras herramientas para descartarlos.

5.2.3. Reportes

- Plasmar en informe ejecutivo las vulnerabilidades encontradas.
- Mostrar cuales son los riesgos existentes.
- Describir el proceso de mitigación de las vulnerabilidades priorizando los hallazgos críticos.
- El responsable de Seguridad de la Información confecciona una matriz de riesgos donde se muestra cuáles son las vulnerabilidades encontradas, los riesgos que implican y su probabilidad de ocurrencia. Adicionalmente elabora un informe con las recomendaciones correspondientes y cómo deben ser aplicadas. Dicho informe se

facilita a los equipos técnicos correspondientes para su mitigación donde se realiza un estudio de factibilidad asociado y se proponen fechas de remediación.

- En caso de no poder implementar la mitigación por incompatibilidad operacional, alta complejidad del cambio o costos, el responsable de seguridad en conjunto con el equipo técnico afectado evalúa métodos alternativos para controlar los posibles riesgos. La aplicabilidad de dichas correcciones no solo es para la infraestructura analizada, se deben identificar oportunidades de mejora en otros equipos con características iguales o parecidas donde se debe evaluar su aplicación para mantener la homogeneidad de la plataforma.

5.2.4. Instalación de Parches Críticos de Seguridad

- Las instalaciones de parches y actualizaciones deben ser realizadas por personal idóneo y capacitado para cumplir esta labor.
- Los parches y actualizaciones deben provenir de una fuente legítima.
- El nivel mínimo de actualización de los parches críticos que las máquinas deben tener es de n-3 (máximo 3 parches pendientes).
- Previo a la instalación de un parche, debe validarse un rollback de la plataforma donde vaya a ser instalado en caso de ser necesaria la restauración a una versión anterior.
- Los parches y actualizaciones deben ser testeados en un ambiente de pruebas para evitar posibles fallos en las aplicaciones y evitar que la información sea inasequible en el tiempo que se requiere. De no contar con un ambiente de pruebas, se deben tomar las medidas necesarias para que la instalación del parche no impacte la operación de INTIZA.
- Registrar y controlar la instalación de parches y actualizaciones para mantener un inventario de los cambios realizados en la plataforma de INTIZA, para ello se deberá tener en cuenta el registro **“RE-SI-11 Gestión de Vulnerabilidades y Parches”**

- La instalación de los parches debe realizarse en horas en las cuales no se afecte la operación y se evite la interrupción del servicio. Esta indicación es considerada en función a que la instalación de parches puede requerir reinicio de aplicaciones o servicios al igual que el sistema operativo.

5.2.5. Excepciones

Toda aquella excepción, conflicto, interpretación o discrepancia de la presente, deberá ser formalmente evaluada, autorizada y aprobada según corresponda por el propietario de la información en cuestión.

5.3. Email Threat Management

El responsable de Seguridad de la Información será responsable de administrar y gestionar el sistema de correo electrónico de toda la organización de forma activa con el objetivo de detectar spam, malware y contenido inapropiado que pudiera poner en riesgo la operación de INTIZA

Todo correo electrónico sospechoso se pondrá en cuarentena para evitar interrupciones en los sistemas informáticos de la compañía o la red de INTIZA.

5.4. Amenazas De Navegación En Internet

El acceso a internet dentro de la red interna de INTIZA y por medio de VPN, posee controles de seguridad implementados para informar a los usuarios sobre sitios potencialmente maliciosos y detener activamente el acceso a sitios maliciosos conocidos.

5.5. Concientización De Seguridad

El responsable de Seguridad de la Información concientizará a los usuarios de la organización sobre incidentes y vulnerabilidades de seguridad con el objetivo de instruir a toda la organización sobre los riesgos que pueden tener un impacto negativo en la organización.

5.6. Auditoría y Control

Los registros (logs) creados por servidores, firewalls, dispositivos de red, programas de control y aplicaciones serán analizados, asegurados y mantenidos durante un período de tiempo para ayudar con la resolución de problemas y las evaluaciones forenses.

6. Referencias

6.1. Normativa Relacionada

Categoría	Título	Código
Procedimiento	Gestión de Vulnerabilidades y Parches	PR-SI-07
Registro	Gestión de Vulnerabilidades y Parches	RE-SI-11

6.2. Definiciones

Término	Descripción
Seguridad de la Información	conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Log	Se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema
Amenaza	Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización.
Vulnerabilidad	Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas.
Malware	O código malicioso, se refiere a un programa que se encuentra de forma encubierto e insertado en otro programa con la intención de destruir los datos, ejecutar programas destructivos o intrusivos, comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones, o sistema operativo.

7. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	01/07/2021	Creación de la Norma de Vulnerabilidades.
1.0	02/05/2022	Aprobado por Comité de Dirección: MI-DI-03- Minuta de Comité de Dirección N° 3

2.0	01/09/2022	Se agregan en documentos relacionados el procedimiento de gestión de vulnerabilidades y parches y el registro de gestión de vulnerabilidades y parches.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06- Minuta de Comité de Dirección N° 6
2.1	01/07/2024	Se revisó el contenido del documento confirmando su vigencia. Se agregó clasificación del documento en el encabezado y se eliminó del pie de página.
2.1	09/08/2024	Aprobado por Comité.