1. Objetivo

Gestionar las vulnerabilidades técnicas que impacten en los sistemas de información del IND, implementando también una gestión sobre los parches de seguridad en los sistemas operativos y aplicativos instalados de los servidores y estaciones de trabajo de la institución.

2. Alcance

Este procedimiento debe ser aplicado por el Departamento de Informática, específicamente al Área Operaciones, como parte de sus responsabilidades en la administración segura de la plataforma TIC.

La gestión de vulnerabilidades y parches de seguridad tiene como especial alcance la plataforma TIC que soporta los productos estratégicos de la institución.

Este procedimiento cubre el control A.12.06.01 de la ISO 27001:2013.

3. Referencias

- Norma NCh-ISO 27001:2013
- Política General de Seguridad de la Información
- Política de Operaciones

4. Roles y responsabilidades

Encargado de Seguridad:

- Velar por el correcto cumplimiento de este procedimiento.
- Administrar las alertas del fabricante y del CSIRT con respecto a los parches de seguridad y las vulnerabilidades técnicas.
- Generar el requerimiento para ejecutar parches de seguridad en servidores.
- Ejecutar la evaluación periódica de vulnerabilidades técnicas en los sistemas de información de la institución.

Jefatura de Departamento de Informática

- Administrar los registros de operación generados a partir de la ejecución de este procedimiento y elaborar el Informe de vulnerabilidades técnicas.

Área de Operaciones TI:

- Coordinar la detección y evaluación de vulnerabilidades técnicas ya sea con proveedor externo o con recursos internos.

- Darle tratamiento a las vulnerabilidades técnicas detectadas en la plataforma TIC de la institución.
- Desplegar los parches de seguridad en los servidores y estaciones de trabajo de la institución.
- Administrar las herramientas que permiten el despliegue de parches de seguridad.
- Resolver vulnerabilidades técnicas detectadas en la plataforma TIC de la institución.

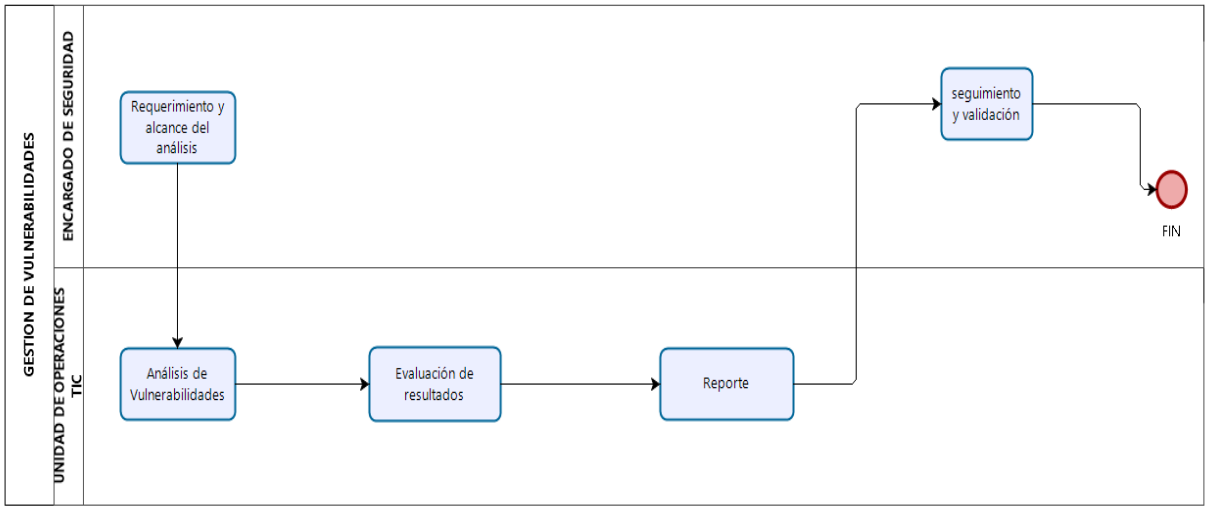
5. Revisión y Evaluación

El presente Procedimiento debe ser objeto de revisión y de evaluación en relación con su correcta aplicación cuando se cumpla un año de su aprobación, o bien, en forma extraordinaria, cada vez que se presente un evento que propicie un ajuste de las declaraciones establecidas en este Procedimiento.

6. Materias específicas que aborda

- NORMA NCh-ISO 27001:2003: define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de una organización.
- Control A.12.06.01: Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información.

7. Descripción del proceso de administración de vulnerabilidades técnicas



8. Matriz del proceso de administración de Vulnerabilidades técnicas

N°	Quién	Que	Cuando	Cómo	Registro
1	Encargado de Seguridad	Definir requerimiento y alcance para el análisis de vulnerabilidades	Una vez al año	Para los sistemas que soportan productos estratégicos, se generará análisis periódicos y/o según demanda, considerando adicionalmente los reportes de vulnerabilidades de servicios externos de monitoreo y del CSIRT de ministerio del interior. El requerimiento se enviará al área de Operaciones TIC.	Inventario de sistemas críticos
2	Área de Operaciones TIC	Análisis de vulnerabilidades	Una vez al año	El análisis lo realizará el área de Operaciones con recursos internos, o con un proveedor externo. Para los ambientes de producción, el análisis de vulnerabilidades debe ser realizado en una ventana horaria determinada, y previa coordinación con los dueños de los sistemas, para evitar impacto en la continuidad operacional.	Logs de las herramientas para análisis de vulnerabilidades
3	Área de Operaciones TIC	Evaluación de resultados	Una vez al año	Análisis de los datos entregados por las herramientas de análisis; evaluación de los riesgos, establecer las medidas de mitigación y la priorización de las mismas.	Reporte de Vulnerabilidades
4	Área de Operaciones TIC	Reporte de resultados del análisis	Una vez al año	Se presenta un informe con los hallazgos junto con los planes de acción, priorizados en virtud los riesgos detectados.	Reporte de Vulnerabilidades
5	Encargado de Seguridad	Seguimiento y validación	Según plan de acción	Seguimiento del cumplimiento de las medidas establecidas en el plan de acción.	Reporte de Vulnerabilidades

9. Registros de Operación

Control	Nombre del Registro	Descripción	Responsable	Periodicidad
A.12.6.1	Informe de vulnerabilidades técnicas	Reporte con el análisis de vulnerabilidades y los planes de acción.	Jefatura del Departamento de Informática.	Anual

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración	Cristian Villalobos Zamora	Encargado PMG Seguridad de la Información	
Responsable de Revisión	Edson Maya Vera	Encargado Área de Operaciones	
Responsable de Revisión y Aprobación	Carola Molina Cecchi	Encargada de Seguridad de la Información	

Control de Cambios

Versión	Fecha	Responsable	Descripción
Versión 1	23-09-2019	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento su aplicación y cumplimiento al PMG-2019 y abordar requerimientos internos del IND.