1. Objetivo

Este documento establece las directrices que garanticen en forma segura la administración de operaciones en los sistemas en producción y la gestión de eventos.

2. Alcance

Este procedimiento aplica a los sistemas de información que soportan los productos estratégicos de la institución, de acuerdo a lo establecido en el Formulario de Definiciones Estratégicas (A1).

Este procedimiento cubre el control A.12.04.01 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

- Comité de Seguridad de la Información:
  - Supervisar la implementación de las actividades que se desprenden del presente procedimiento.
- Jefatura del Departamento de Informática:
  - Proveer los recursos necesarios para la implementación del monitoreo y gestión de eventos en la plataforma TIC del IND
- Área de Operaciones del Departamento de Informática:
  - Administrar las herramientas que permiten llevar a cabo la gestión de eventos
  - Monitorear los eventos que puedan afectar la seguridad de la plataforma.
  - Generar reportes periódicos con el resultado del monitoreo de eventos.

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. Difusión

El presente Procedimiento será difundido por medio de su publicación en la sección "Seguridad de la Información" de la intranet institucional.

7. Materias específicas que aborda

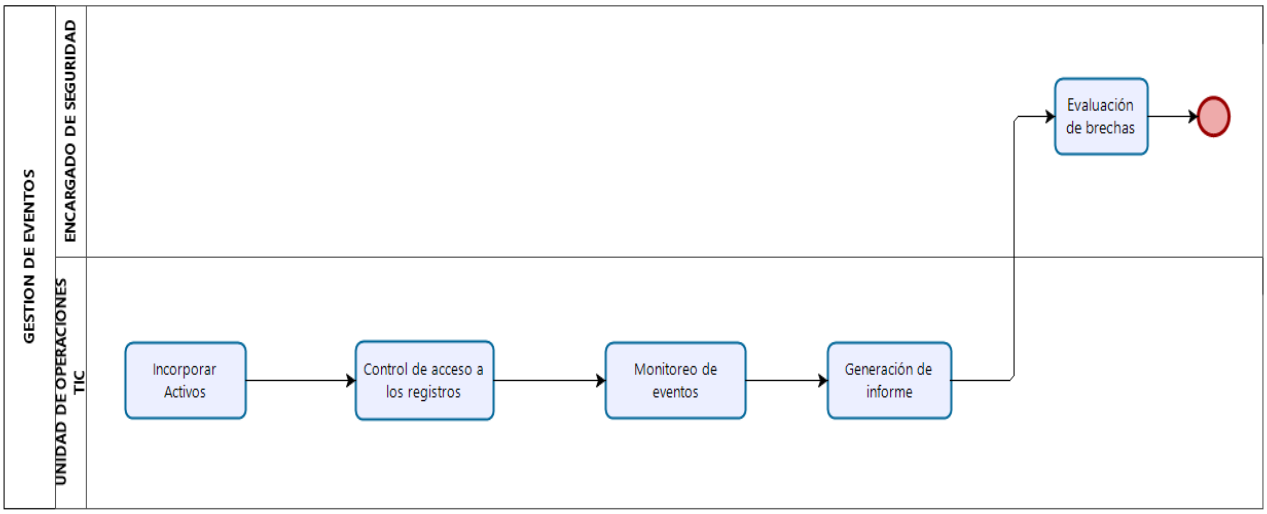
- NORMA NCh-ISO 27001:2003: define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de una organización.
- Control A.12.04.01: Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, fallas, excepciones y eventos de seguridad de la información.

8. Formularios / Formatos Aplicables

- NA

9. Descripción del proceso de Gestión de Registro de Eventos

9.1 Flujo del procedimiento de gestión de eventos.



10. Matriz de proceso de Gestión de Eventos.

N°	Quién	Que	Cuando	Cómo	Registro
1	Área de Operaciones	Incorporar activos	Cuando se incorporen nuevos sistemas o activos de información	En sistema de monitoreo de eventos se deben incorporar los servidores y equipos de comunicaciones que tengan un alto impacto en los productos estratégicos de la institución. La documentación de apoyo será el instructivo de administración del SIEM.	Logs del SIEM
2	Área de Operaciones	Control de acceso a los registros	Diariamente	Mantener un acceso restringido para la plataforma de monitoreo. Generar un registro actualizado de las cuentas y usuarios con privilegios.	Consola de administración del SIEM
3	Área de Operaciones	Monitoreo de eventos	Diariamente	Revisión periódica de los eventos almacenados en la base de datos del SIEM. Priorizar aquellos que requieran alguna acción inmediata, alertar posibles amenazas al encargado de Ciberseguridad.	Logs del SIEM
4	Área de Operaciones	Generación de informe	Mensualmente	Generar informe mensual con el resultado de los eventos gestionados por el SIEM, destacando las debilidades, amenazas y brechas de seguridad detectadas en el período, junto con los planes de acción llevados a cabo para mitigarlos.	Informe de eventos
5	Encargado de Seguridad	Evaluación de brechas	On Demand	Cada vez que se identifique una brecha de seguridad importante por el monitoreo de la plataforma, y ante la generación del informe evaluando los resultados del mismo. Generar los planes de acción necesarios para mitigar los riesgos identificados.	Informe de eventos

11. Registros de Operación

Control	Nombre del Registro	Descripción	Responsable	Periodicidad
A.12.4.1	Informe de eventos	Informe mensual con el resultado de los eventos gestionados por el SIEM.	Jefatura del Departamento de Informática.	Mensual

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.