1. RESUMEN

La Política de Gestión de Incidentes establece directrices para el manejo y la administración adecuados de los incidentes de seguridad que afectan a los activos de información. Además, se trata de un documento esencial, detallado y sujeto a revisiones continuas, que resulta fundamental para que el personal o colaboradores de la empresa tomen las acciones necesarias en caso de incidentes de seguridad.

2. OBJETIVO

La política tiene como objetivo definir directrices generales para la gestión de incidentes de seguridad de la información, con el propósito de prevenir y mitigar el impacto que pueda tener la materialización de cualquier amenaza sobre los activos de información.

3. ALCANCE

Esta política es aplicable a todo el personal o colaboradores de la organización que cuenten con autorización para acceder a los recursos de los Sistemas de Información o para manejar e interactuar con los activos de información propiedad de la organización.

4. POLÍTICA

Es responsabilidad del personal o colaboradores de la organización conocer la política y su alcance, así como tener en cuenta el registro de incidencias en el Sistema de Gestión de Tickets de la organización. En este sentido, las normas que forman parte de la Política de Gestión de Incidentes de Seguridad son:

4.1 NORMAS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.1.1 NORMA N°1: SISTEMA DE GESTIÓN DE INCIDENTES

- La organización dispone de un Sistema de Gestión de Incidentes de Seguridad de la Información, integrado en el Sistema de Gestión de Tickets. Este sistema mantiene un registro detallado de todos los incidentes de seguridad, junto con un inventario histórico que incluirá: la persona que reportó el incidente, la descripción del mismo, el activo de información comprometido, las acciones preliminares realizadas, entre otros elementos esenciales para una gestión adecuada y una respuesta inmediata al incidente.

4.1.2 NORMA N°2: OBLIGACIÓN DE LA ORGANIZACIÓN

- La organización implementará medidas de seguridad efectivas para garantizar la protección de sus activos de información críticos.
- La organización analizará los eventos de seguridad relacionados con los activos de información para identificar, verificar y determinar si se trata de un incidente de seguridad de la información.
- La organización aplicará procedimientos de respuesta ante incidentes para mitigar o controlar los riesgos de seguridad que afecten a los activos de información.
- La organización llevará a cabo investigaciones continuas sobre los incidentes de seguridad de la información, tanto los que afecten como los que no afecten a los activos de información, y los documentará para proporcionar información relevante al personal, con el fin de prevenir futuros incidentes.

- La organización considerará realizar actividades post-incidente para reducir las consecuencias derivadas de una amenaza sobre los activos de información, asegurando que todo el proceso sea debidamente documentado.

4.1.3 NORMA N°3: OBLIGACIÓN DEL PERSONAL DE LA ORGANIZACIÓN

- El personal o colaboradores de la organización son responsables de informar de manera oportuna cualquier evento o incidente relacionado con los activos de información de la organización.

5. CUMPLIMIENTO DE POLÍTICA

5.1 MEDICIÓN DEL CUMPLIMIENTO

La Organización, especialmente el Oficial de Seguridad de la Información (OSI) y el responsable del riesgo de cada activo de información, se encargarán de verificar el cumplimiento de esta política utilizando diversos métodos, como pruebas simuladas de amenazas a los activos de información u otros enfoques que la organización considere adecuados.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: