Política de Seguridad

Protección de seguridad de la información y datos personales

Contenido

1 Introducción

La presente Política Pública de Seguridad y Privacidad de la Información establece los principios, compromisos y lineamientos generales mediante los cuales CNMM protege la información y los datos personales que gestiona, en cumplimiento de su misión, sus objetivos estratégicos y sus obligaciones legales y contractuales.

Esta política se publica con el fin de garantizar la transparencia frente a clientes, usuarios, proveedores, autoridades y demás partes interesadas, y constituye el marco de referencia para la implementación, operación y mantenimiento del sistema.

CNMM adopta esta política conforme a las mejores prácticas internacionales, alineándose con el Esquema Nacional de Seguridad (ENS).

2 Emisión y revisión de la política

La presente política entra en vigor a partir de su aprobación por la alta dirección y será revisada periódicamente para garantizar su adecuación y mejora continua.

3 Objetivo

Este documento es de carácter público y refleja el compromiso de CNMM con la seguridad de la información y la protección de la privacidad.

El objetivo de la presente política es establecer el compromiso público de CNMM con la adecuada gestión de la seguridad de la información y la protección de los datos personales, asegurando los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad, así como el respeto de los derechos de los titulares de la información

4 Alcance

Esta política aplica a toda la información y a todos los datos personales tratados por CNMM, independientemente de su naturaleza, formato, medio de almacenamiento o canal de transmisión.

Es de obligatorio cumplimiento para:

- Gerencia,
- Empleados del CNMM,
- Proveedores,
- Personas físicas o jurídicas que accedan o utilicen los sistemas de información de CNMM.

El alcance incluye procesos, activos de información, infraestructuras tecnológicas, servicios en la nube, redes, aplicaciones y servicios gestionados directa o indirectamente por CNMM.

5 Marco normativo y de referencia

La presente política se fundamenta en los siguientes marcos normativos y de buenas prácticas, con especial alineación al Esquema Nacional de Seguridad Nivel Alto:

- Esquema Nacional de Seguridad (ENS), Real Decreto 311/2022, Nivel Alto.
- Legislación vigente en materia de protección de datos personales (LOPDGDD y RGPD), ciberseguridad, continuidad del negocio y seguridad de la información aplicable a CNMM.

6 Glosario

Para efectos de esta política, se adoptan, entre otros, los siguientes conceptos:

- Activo de información: información o recurso que tiene valor para CNMM y debe ser protegido.
- Confidencialidad: propiedad que garantiza que la información no sea divulgada a personas no autorizadas.
- Integridad: propiedad que asegura la exactitud y completitud de la información.
- Disponibilidad: propiedad que garantiza que la información esté accesible cuando sea requerida.
- Riesgo: posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo.
- Incidente de seguridad de la información: evento que compromete o puede comprometer la seguridad o la privacidad de la información.
- Datos personales: cualquier información vinculada o que pueda asociarse a una persona física identificada o identificable.

7 Política general de seguridad y privacidad de la información

La información es considerada uno de los principales activos de CNMM y, como tal, debe ser protegida mediante controles administrativos, técnicos y organizativos apropiados.

CNMM orienta sus esfuerzos a preservar la seguridad y privacidad de la información durante todo su ciclo de vida, promoviendo una cultura de seguridad, responsabilidad y cumplimiento entre todas las partes interesadas.

8 Políticas específicas de seguridad y privacidad de la información

8.1 Criterios generales

- El acceso a los sistemas de información se gestiona bajo el principio de mínimo privilegio.
- La administración de accesos y perfiles es responsabilidad de las áreas autorizadas.
- Los servicios en la nube solo se utilizarán cuando existan garantías contractuales y técnicas adecuadas.
- Los activos tecnológicos serán gestionados durante todo su ciclo de vida.

8.2 Uso de internet

El uso de internet y de los servicios de red debe estar alineado con las funciones del negocio, respetando las restricciones y controles de seguridad establecidos por CNMM.

8.3 Bases de datos

Las bases de datos serán administradas de forma segura, garantizando su integridad, confidencialidad y disponibilidad, y aplicando criterios de retención y eliminación conforme a los fines definidos.

8.4 Copias de seguridad (backup)

CNMM implementa mecanismos de respaldo periódico de la información crítica, garantizando su recuperación ante incidentes, fallos o desastres.

8.5 Acceso remoto

El acceso remoto a los sistemas de información se realizará únicamente mediante mecanismos seguros, autenticados y autorizados.

8.6 Política de autenticación multifactor

El acceso a sistemas críticos requerirá mecanismos de autenticación robustos, incluyendo autenticación multifactor cuando aplique.

8.7 Política de equipos de trabajo

El uso de dispositivos móviles para el tratamiento de información corporativa estará regulado y sujeto a controles de seguridad.

8.8 Empleados

Todas las personas con acceso a la información de CNMM son responsables de cumplir esta política y las normas internas asociadas.

8.9 Seguridad en la nube

La información almacenada o procesada en la nube será protegida mediante controles de cifrado, monitoreo y respaldo.

8.10 Gestión de incidentes de seguridad y privacidad

CNMM dispone de procedimientos para detectar, reportar, gestionar y aprender de los incidentes de seguridad y privacidad.

8.11 Acuerdos de confidencialidad

Todas las personas que accedan a información de CNMM deberán suscribir acuerdos de confidencialidad y compromisos de seguridad y privacidad.