CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de concientización y formación

Versión 1.0

APROBACIONES

Elaborado por:	Revisado por:	Aprobado por:
<Nombre>	<Nombre>	<Nombre>
<Cargo>	<Cargo>	<Cargo>
<Firma>	<Firma>	<Firma>

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	Diciembre 2021	Versión Inicial

Contenido

1. Introducción

1.1 Autoridad

El Centro Nacional de Seguridad Digital fue creado el 9 de enero del 2020, mediante Decreto de Urgencia N° 007-2020, es el encargado de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. También es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital.

1.2 Propósito

El propósito de esta política es asegurar que, en todo momento, los empleados conocen, entienden y cumplen las normas y las medidas de protección en materia de ciberseguridad y seguridad de la información adoptadas, advirtiéndoles de los riesgos que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.

1.3 Alcance

Esta política se aplica a todos los empleados y afiliados de la organización.

2. Política

2.1 Se debe documentar y difundir las normas de ciberseguridad y seguridad de la información de la organización para que estén siempre accesibles.

2.2 Las normas de ciberseguridad y seguridad de la información de la organización deben estar correctamente documentadas y al alcance de todo el personal en todo momento.

2.3 Se debe elaborar o revisar el plan de formación para elevar el nivel de seguridad digital.

2.4 Se debe desarrollar programas de formación y concientización especializados para ciertos perfiles de empleados en ciberseguridad y seguridad de la información.

2.5 Se debe elaborar una actividad formativa introductoria para los nuevos empleados.

2.6 Se debe desarrollar y aplicar programas de formación en ciberseguridad y seguridad de información adecuados a los distintos puestos de trabajo.

2.7 Los empleados deben realizar cursos o charlas de concientización, al menos dos veces al año.

2.8 Se debe comprobar la asimilación del conocimiento adquirido por los empleados.

2.9 Se debe evaluar el aprendizaje obtenido por los empleados, para determinar el grado de concientización y formación alcanzado.

2.10 Se debe promover una cultura de seguridad de la información.

2.11 Se debe coordinar el uso de la plataforma del Centro de Conocimiento Digital en todas las entidades.

3. Cumplimiento de políticas

3.1.1 Medición de cumplimiento

Se verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la póliza.

3.1.2 Excepciones

Cualquier excepción a la política debe ser aprobada con anticipación.

3.1.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo.