CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de uso de internet

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 definir lo que está permitido o no, a fin de que la organización pueda atender las necesidades esenciales para que los colaboradores puedan desempeñar sus funciones en un ambiente de calidad.

1.3 Alcance

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

2. Política

2.1 El acceso a internet debe ser solo de interés laboral y no personal.
2.2 Todos los usuarios deben seguir los principios corporativos con respecto al uso de los recursos y ejercer un buen juicio en el uso de Internet.
2.3 El uso aceptable de internet debe incluir la comunicación entre empleados y no empleados con fines comerciales.
2.4 El uso aceptable de internet debe incluir el soporte técnico de TI para descargar actualizaciones y parches de software.
2.5 El uso aceptable de internet debe incluir la revisión de posibles sitios web de proveedores para obtener información sobre productos.
2.6 El uso aceptable de internet debe incluir información reglamentaria o técnica de referencia.
2.7 El uso aceptable de internet debe incluir temas de investigación.
2.8 No se debe ingresar a páginas con temas de violencia, pornografías u otros contenidos inapropiados.
2.9 Se debe mantener en todo momento la confidencialidad de sus datos de acceso a internet, siendo el único responsable del buen o mal uso de sus datos de acceso.
2.10 Se debe notificar de manera inmediata al área de Soporte Técnico cualquier uso no autorizado de su cuenta o cualquier otra observación de seguridad.
2.11 Se debe usar herramientas de software instaladas que habiliten servicios potencialmente riesgosos para la organización.
2.12 Solo se debe manejar correos electrónicos institucionales.
2.13 El uso de los datos confidenciales de la organización debe ser de acceso restringido.
2.14 Se debe usar sitios web oficialmente permitidos (https).
2.15 Toda persona que incumpla esta política debe estar sujeto a sanciones disciplinarias.

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.