CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de medios extraíbles

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 minimizar el riesgo de pérdida o exposición de información confidencial mantenida en "medios extraíbles".

1.3 Alcance

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

2. Política

2.1 Si es posible se debe restringir el uso de medios extraíbles.

2.2 Solo si es absolutamente necesario de debe utilizar dispositivos de medios extraíbles.

2.3 Se debe utilizar los medios extraíbles de forma segura y protegida (información confidencial).

2.4 Se debe utilizar los dispositivos de medios extraíbles solo con fines laborales.

2.5 Se debe asegurar que la estación de trabajo no tenga habilitada la función de ejecución automática.

2.6 Se debe limitar la copia de archivos mediante medios extraíbles, a menos que sea necesario o haya sido autorizado, se recomienda tener un sistema DLP (prevención de pérdida de datos).

2.7 Se debe escanear los medios extraíbles en busca de malware antes de transferir información.

2.8 Se debe aplicar protección con contraseña al medio extraíble de almacenamiento.

2.9 Se debe cifrar cualquier información contenida en un dispositivo de almacenamiento extraíble.

2.10 Los empleados deben informar sobre los dispositivos de medios extraíbles perdidos.

2.11 Los medios extraíbles deberán estar prohibidos en las redes misionales, así por ejemplo en una organización que se dedica a la salud no debería permitirse el uso de estos dispositivos en las estaciones de trabajo que intervienen en los servicios de salud.

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.