CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política para uso de dispositivos móviles

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 garantizar que la información de la organización no se vea comprometida.

1.3 Alcance

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

2. Política

2.1 Los medios de almacenamiento de los dispositivos móviles propios deben estar cifrados.

2.2 Se debe reportar la pérdida o extravío de dispositivos propios de la organización de forma inmediata a la toma de conocimiento, siguiendo los pasos detallados en un procedimiento formal.

2.3 Las aplicaciones instaladas en el dispositivo deben ser obtenidas por canales oficiales y con el licenciamiento debido.

2.4 Se debe implementar, para los dispositivos que lo soporten, instrumentos y herramientas técnicas (hardware, software) que permitan bloquear y/o borrar la información de forma remota.

2.5 Se debe contar con procedimientos para la reutilización y/o eliminación de dispositivos (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible anteriormente almacenada.

2.6 Se debe establecer a qué nivel de control y monitorización están sometidos dichos dispositivos y las medidas y posibles sanciones aplicables cuando se produce algún tipo de abuso o infracción por parte de los trabajadores.

2.7 Se debe contar con mecanismos de protección ante código malicioso, en caso de que corresponda.

2.8 Se debe hacer un inventario de los dispositivos móviles propios de la organización.

2.9 Se debe usar controles de acceso (autenticación con contraseñas, doble factor, VPN, entre otros), contar con bloqueo mediante contraseña u otro medio robusto de autenticación.

2.10 No se debe exponer el equipo a altas temperaturas.

2.11 Se debe supervisar el uso de aplicaciones de almacenamiento en la nube.

2.12 Se debe desactivar en el teléfono la búsqueda de redes Wi-fi públicas y dispositivos vías bluetooth.

2.13 Se debe llevar a cabo auditorías periódicas para asegurar el cumplimiento de la política.

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.