CENTRO NACIONAL DE SEGURIDAD DIGITAL

# Política de aplicaciones permitidas

**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 controlar que siempre se use software autorizado en la organización, y que haya sido adquirido de forma legal.

## 1.3 Alcance

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

## 2. Política

2.1 Se debe mantener un registro actualizado de las licencias disponibles del software autorizado. El registro deberá almacenar al menos la siguiente información: nombre y versión del producto; autor; fecha de adquisición; vigencia de la licencia; tipo de licencia; número de usuarios permitidos por licencia; número de licencias adquiridas por cada software; facturas o comprobantes de compra; ubicación física del producto.

2.2 Se debe nombrar y autorizar al personal técnico que se encargará de la instalación, actualización y eliminación del software de los equipos de la organización. En caso el personal encargado sea externo, se debe documentar y notificar la autorización y la operativa para instalar, actualizar, revisar y eliminar software legal de forma autónoma, para ello se deberá utilizar una cuenta de administrador diferente a la del usuario habitual.

2.3 No se debe permitir la instalación ni la actualización de software a través de enlaces de webs o correos cuyo origen no sea completamente seguro.

2.4 Se debe remarcar que el software instalado en los equipos debe estar correctamente actualizado.

2.5 Se debe informar al personal de la organización de las sanciones derivadas del uso no autorizado de software.

2.6 Se debe mantener un repositorio donde se encuentre todo el software autorizado y sus correspondientes credenciales de instalación.

2.7 Se debe garantizar en todo momento que los programas instalados en cualquier dispositivo (corporativo y no corporativo) están debidamente autorizados y disponen de las licencias necesarias.

2.8 Es recomendable que los usuarios lean y comprendan los términos y condiciones de las instalaciones de aplicaciones permitidas.

2.9 No se debe realizar copias del software puesto a disposición sin el debido consentimiento.

2.10 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.