CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de instalación de software

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 describir los requisitos en torno al software de instalación en dispositivos informáticos.

1.3 Alcance

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

2. Política

2.1 Todo el software instalado en los sistemas, debe cumplir con las pautas de licencia de software aplicables.

2.2 La especificación de software de prueba también debe ser registrada previamente como tal.

2.3 La especificación de software de prueba también debe seguir procedimientos y controles respectivos.

2.4 Todas las licencias deben actualizarse anualmente.

2.5 Los empleados no deben instalar software en los dispositivos.

2.6 El software debe seleccionarse de una lista de software aprobada.

2.7 El personal de tecnología debe obtener información, rastrear las licencias y probar el nuevo software.

2.8 El personal debe reportar si se detecta conflictos y/o compatibilidad después de instalado el software.

2.9 El software instalado no debe entrar en conflicto con las aplicaciones y los controladores de dispositivos existentes.

2.10 Todos los hosts basados en PC deben ser protegidos por antivirus aprobado, antes de la conexión de red.

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.