CENTRO NACIONAL DE SEGURIDAD DIGITAL

# Política de actualización 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 revisar la existencia de actualizaciones y parches de seguridad para el software instalado. Y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en los equipos de forma segura y controlada.

## 1.3 Alcance

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

## 2. Política

2.1 Se debe realizar un inventario del software y firmware instalado, ya que pueden descubrirse errores o mejoras de funcionalidad.

2.2 Se debe realizar un listado del software actualmente existente en la organización, para incluirlo en el plan de actualizaciones.

2.3 Se debe determinar el momento específico para ejecutar las actualizaciones, de este modo no interferir con las operaciones de la organización.

2.4 Se debe usar los canales de alerta y los procedimientos oportunos para detectar e instalar las actualizaciones correspondientes.

2.5 Antes de la actualización se debe considerar la utilidad de las nuevas mejoras y la gravedad los errores que subsanan, así como los requisitos hardware/software necesarios.

2.6 Se debe instalar actualizaciones provenientes de fuentes confiables.

2.7 Se debe revisar las características y los requisitos de las actualizaciones y parches antes de instalarlos.

2.8 Se debe analizar y contrastar en un entorno de pruebas las actualizaciones que se desea instalar.

2.9 Se debe contar con los mecanismos y procedimientos adecuados para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.

2.10 Se debe utilizar herramientas de autodiagnóstico para detectar software no actualizado en los equipos.

2.11 Se debe tener configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad.

2.12 Se debe registrar cada una de las actualizaciones y parches que se instala.

# 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.