CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de copias de seguridad

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 las copias de seguridad es restaurar un sistema a un estado actual (a partir de la fecha de la copia de seguridad más reciente) en caso de falla del sistema.

1.3 Alcance

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

2. Política

2.1 La organización debe contar con copias instantáneas a los sistemas operativos, para poder regresar el sistema operativo a una fecha anterior a la de un incidente.
2.2 La copia de seguridad se debe realizar durante la noche y deberá ser comprobada.
2.3 Las copias de seguridad tendrán una retención en función a los dispositivos legales vigentes.
2.4 La responsabilidad de las copias de seguridad de los computadores personales recaerá en el usuario final.
2.5 Se debe mantener un inventario de activos de información (software, datos, soportes, responsables, ubicación).
2.6 Se debe clasificar los activos de información e identificar los necesarios (críticos).
2.7 Se debe controlar el acceso a las copias de seguridad (personal autorizado).
2.8 Se debe hacer copias de seguridad de la información crítica de la organización.
2.9 Se debe realizar copias de seguridad al menos 1 vez al día, según sea el caso.
2.10 Se debe hacer copias de seguridad completa, incremental o diferencial (según se dé el caso).
2.11 Se debe guardar al menos una copia completa fuera de la organización.
2.12 Se debe guardar las copias de seguridad en una caja ignífuga y bajo llave.
2.13 Se debe realizar copias de seguridad en la nube.
2.14 Se debe elaborar y aplicar los procedimientos de copia y restauración.
2.15 Se debe comprobar que las copias estén bien realizadas y que pueden restaurarse, esto se debe evidenciar con pruebas de restauración de backups que deberán estar documentadas.
2.16 Antes de hacer la copia se debe revisar que el soporte sea el adecuado (tasa de transferencia, capacidad, etc.) y que se encuentre en buen estado.
2.17 Se debe etiquetar los soportes para realizar las copias de seguridad.
2.18 Se debe llevar un registro de los soportes sobre los que se haya realizado alguna copia de seguridad.
2.19 Cuando se desechan los soportes utilizados para las copias de seguridad, se debe destruir de forma segura.
2.20 Se debe cifrar las copias de seguridad que contenga información confidencial y las que se suba a la nube.
2.21 Se debe cifrar de manera obligatoria toda copia de seguridad que salga del local principal.

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.