CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de almacenamiento en la nube

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 establecer en qué casos se permite utilizar el almacenamiento en la nube y mantener de modo seguro la información almacenada en la nube, especificando reglas, criterios y procedimientos que deben seguir todos los empleados que usen estos servicios.

1.3 Alcance

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

2. Política

2.1 Se debe informar a los empleados sobre si se permite o se prohíbe el uso de servicios de almacenamiento en nube públicas.

2.2 Se debe elaborar una lista donde los empleados pueden consultar qué servicios de almacenamiento en la nube están permitidos y cuáles no.

2.3 Se debe evitare el uso de servicios de almacenamiento que no consideremos seguros.

2.4 Se debe informar al personal sobre el procedimiento de borrado adecuado para los repositorios de información en la nube.

2.5 Se debe informar a los empleados del tipo de información que pueden almacenar en la nube.

2.6 Se debe informar a los empleados si la información almacenada en la nube necesita ser cifrada.

2.7 Se deberá incluir la información almacenada en la nube cifrada en la política de clasificación de la información.

2.8 Se debe valorar las ventajas e inconvenientes antes de almacenar las copias de seguridad en la nube.

2.9 Se debe contratar un servicio de almacenamiento en la nube que cumpla con los criterios organizativos y obligaciones legales.

2.10 Se debe considerar como criterios de seguridad específicos la garantía de confidencialidad, disponibilidad de la información, copias de seguridad, entre otros.

2.11 Se debe conocer la política de seguridad del proveedor de servicios de almacenamiento en la nube.

2.12 Se debe conocer las seguridades técnicas que ofrece la nube y éstas deberán ser evaluadas por el área responsable de TI en la organización.

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.