CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de clasificación de la información

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 Clasificar los activos de información para garantizar una eficaz gestión de su seguridad con criterios de confidencialidad, disponibilidad e integridad.

1.3 Alcance

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

2. Política

2.1 Se debe elaborar un inventario detallado de los activos de información de la organización.

2.2 Se debe considerar registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes son sus responsables, etc.

2.3 Se debe etiquetar los activos de información según los criterios de seguridad establecidos.

2.4 Se debe establecer una lista con todos los tratamientos de seguridad de la información.

2.5 Se debe considerar dentro de la lista de tratamientos de seguridad de la información las herramientas de cifrado, sistemas de copias de seguridad, sistemas de control de acceso, entre otros.

2.6 Se debe asignar los tratamientos de seguridad oportunos para cada tipo de información.

2.7 Se debe aplicar los tratamientos de seguridad oportunos para cada tipo de información.

2.8 Se debe realizar auditorías de comprobación al menos dos veces al año.

2.9 Se debe incluir las políticas de almacenamiento en la nube.

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.