CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de transferencia de información y datos

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 mantener la seguridad de la información y los datos transferidos, dentro de la organización y con cualquier entidad externa.

1.3 Alcance

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

2. Política

2.1 Se debe autenticar la identidad y autorización del destinatario para una transferencia de información de forma segura.
2.2 Se debe utilizar un proceso de transferencia seguro aprobado.
2.3 Se debe proteger los datos confidenciales.
2.4 Se debe cifrar los datos.
2.5 Debe existir un acuerdo de procesamiento de datos entre las organizaciones para el propósito especificado.
2.6 Los usuarios pueden intercambiar información confidencial de forma segura, pero debe ser dentro de la organización o con otros usuarios que se encuentren dentro del límite de correo electrónico seguro.
2.7 Si los usuarios necesitan intercambiar información de forma segura fuera del límite de correo electrónico seguro, deben utilizar el cifrado.
2.8 Debe usarse el cifrado para intercambiar datos confidenciales como parte de un flujo de trabajo acordado.
2.9 Los usuarios deben seguir las políticas locales de gobernanza de la información que se establezcan localmente para el envío de datos confidenciales.
2.10 Las soluciones de correo electrónico deben utilizar las comprobaciones pertinentes.
2.11 Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificadas, revisadas y documentadas periódicamente.
2.12 Se debe contar con los medios físicos o técnicos adecuados para la protección de datos.
2.13 Se debe monitorear los flujos de información y datos en toda transferencia.
2.14 Se debe identificar los enlaces de red asociados y se cuenta con la protección adecuada.
2.15 Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y partes externas.
2.16 La información relacionada con la mensajería electrónica debe estar debidamente protegida.

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.