CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de continuidad de negocio

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 diseñar y probar un plan de continuidad de negocio, el cual permita recuperar en un plazo razonable la operativa habitual de la organización para garantizar la continuidad de negocio.

1.3 Alcance

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

2. Política

2.1 Se debe planificar la continuidad de negocio como parte de la seguridad de la información.

2.2 Las áreas de negocio de la organización deben identificar y acordar la importancia de su tecnología de la información.

2.3 Se debe Implementar la continuidad de negocio, basados en las áreas de negocio de la organización.

2.4 Se debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de negocio durante una situación adversa.

2.5 La organización debe tener redes alternativas, portadores de comunicaciones y rutas de transmisión para sus sitios y servicios críticos.

2.6 Se debe verificar, revisar y evaluar la continuidad de negocio.

2.7 Las áreas de negocio de la organización verificarán lo establecido e implementado controles de continuidad de la seguridad de la información a intervalos regulares con el fin de garantizar que son válidos y eficaces en situaciones adversas. Esto sucederá a través de pruebas de continuidad del negocio planificadas y eventos no programados.

2.8 Los incidentes importantes y significativos deben incluir un análisis de la causa raíz para garantizar que se toman las medidas correctivas adecuadas para proteger contra incidentes futuros y mejorar las medidas de seguridad.

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.