CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de gestión de riesgos

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 los requisitos mínimos para mantener la "gestión de riesgos" dentro de la organización.

1.3 Alcance

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

2. Política

2.1 La gestión de riesgos debe adoptarse durante los proyectos, siguiendo el sistema políticas de seguridad y se pueden utilizar para evaluar cambios.
2.2 Se debe llevar a cabo un proceso de gestión de riesgos para todos los sistemas.
2.3 Los proyectos del ciclo de vida deben seguir el proceso de riesgo definido por la gestión de proyectos.
2.4 Los propietarios responsables del riesgo deben ser identificados.
2.5 Cuando existen riesgos posteriores a la implementación, se deben identificar los propietarios del riesgo.
2.6 Los riesgos cibernéticos pueden aplicarse a todos los niveles de gestión de riesgos según el sistema o servicio.
2.7 La identificación de riesgos se llevará a cabo identificando los activos de la organización.
2.8 Una vez definido el alcance de la evaluación de riesgos en la identificación del activo, cada activo se emparejará con una lista de conjuntos de amenazas claramente articulados.
2.9 Los riesgos se identificarán en función de los activos, las amenazas y las vulnerabilidades que utilicen las amenazas.
2.10 Se debe seguir un proceso de evaluación de riesgos cuantitativo donde la probabilidad de cada riesgo se puntúa de acuerdo a una escala predefinida.
2.11 De manera similar, se debe definir una escala para el impacto de la ocurrencia del evento.
2.12 Para cada riesgo, el producto de probabilidad e impacto proporcionará la puntuación de riesgo. Establecido los riesgos de puntuación se clasifican en tres categorías para atender la urgencia de tratamiento del mismo.
2.13 El resultado de la evaluación será cómo se pueden progresar los requisitos de seguridad.
2.14 El proceso de gestión del riesgo se evaluará al menos una vez al año para ver cómo funciona y puede ser mejorado.
2.15 Siguiendo el apetito de riesgo de la organización, cualquier riesgo sobre el valor definido debe ser tratados por los equipos de proyecto u operación.
2.16 Se debe desarrollar e implementar un plan de tratamiento de manejo específico (planes de acción), que incluyen consideraciones de costos.
2.17 Dentro del plan de tratamiento de riesgos, las opciones de tratamiento son modificación, retención, evitación o intercambio, con el objetivo de reducir los riesgos residuales y tener un tratamiento satisfactorio.
2.18 El evaluador de riesgos se comunicará y consultará con las partes interesadas internas y externas, según corresponda, en cada etapa del proceso general.
2.19 El evaluador de riesgos realizará informes de riesgos según sea necesario para tomar una decisión adecuada.

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.