Instituto Nacional de Deportes Gobierno de Chile	**POLITICA DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN** Página: Página 1 de 6 Versión : 1 Fecha Aprobación : 16 de mayo de 2019 Código: IND-SSI-A17-POL-01

1. OBJETIVO

Entregar las directrices para determinar los requisitos para la seguridad de la información y la continuidad de la administración de la seguridad de la información ante situaciones adversas, velando por que la Seguridad de la Información se implementa y se opera de acuerdo a las políticas y procedimientos vigentes en el IND.

2. ALCANCE

Esta política aborda la planificación de la continuidad de la seguridad de la información dentro del proceso de administración de recuperación tecnológica ante desastres, en aquellos sistemas que dan soporte a los procesos de provisión vigentes en el IND, de acuerdo a lo establecido en el Formulario de definiciones Estratégicas (A1).

3. MATERIAS ESPECÍFICAS QUE ABORDA

- A.17.01.01 Planificación de la continuidad de la seguridad de la información

4. ROLES Y RESPONSABILIDADES

- Comité de Seguridad de la Información
  - Supervisar la implementación y difusión de las recomendaciones y normas establecidas en la presente política.
- Encargado/a de Seguridad de la Información
  - Velar por el cumplimiento e implementación de esta política.
  - Velar por mantener la seguridad de la información durante la administración del incidente.
- Encargado/a de Ciberseguridad
  - Apoyar al Encargado de Seguridad en la planificación e implementación de la continuidad de la seguridad.
- Jefatura Unidad Coordinación Informática
  - Establecer los requisitos de seguridad de la información que deben considerarse dentro del proceso de administración de recuperación tecnológica ante desastres.

5. REVISIÓN Y EVALUACIÓN

La presente Política debe ser objeto de revisión y de evaluación en relación con su correcta aplicación cuando se cumplan dos años de su aprobación, o bien, en forma extraordinaria, cada vez que se presente un evento que propicie un ajuste de las declaraciones establecidas. En ambos casos, estas revisiones y evaluaciones serán realizadas en las sesiones del Comité de Seguridad de la Información.

6. DIFUSIÓN

La presente Política debe ser difundida por medio de su publicación en la sección "Seguridad de la Información" de la intranet institucional.

7. DEFINICIONES

- Desastre: Evento catastrófico y repentino que anula la capacidad de la CNE para llevar a cabo sus procesos críticos. Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación o la incapacidad de los empleados para acceder a las instalaciones, generado por algún tipo de desastre natural, una contingencia sanitaria, una huelga, etc.
- Recuperación tecnológica: Proceso que comprende aquellas actividades que se necesitan realizar para recuperar una condición o capacidad de procesamiento en su operación normal aplicados a las comunicaciones, los servidores, las aplicaciones y los datos.

8. POLITICA

8.1 Planificación de la continuidad de la seguridad en la información.

Los controles de seguridad de la información que se han implementado en la DT deben seguir funcionando durante una situación adversa, y debe ser el Encargado de Seguridad de la Información quien lidere el proceso de aseguramiento de continuidad de la seguridad de la información, junto al equipo que él designe, dependiendo de las características de la situación.

8.2 Evaluación y pruebas de estrategias de continuidad

- Una vez por año, la Jefatura de la Unidad Coordinación Informática en conjunto con el Encargado de Seguridad y el Encargado de Ciberseguridad deben evaluar, proponiendo distintos escenarios de contingencia, los controles de seguridad relacionados con el control de acceso lógico, las políticas de respaldo y restauración, los controles antivirus, control de

cambios, monitoreo de la plataforma, la disponibilidad de los enlaces de red y respuesta ante incidentes, de manera prioritaria, coordinando la revisión en terreno con el área y/o proveedor involucrado según sea el caso.

- El Encargado de Seguridad de la Información debe identificar aquellos hallazgos que podrían afectar al normal funcionamiento del control implementado y proponer acciones, en conjunto con el Encargado de Ciberseguridad, para el tratamiento del hallazgo encontrado, el cual puede ser un control compensatorio, o la optimización de un control normativo ya implementado.

- Posteriormente, el Encargado de Seguridad debe coordinar con el área responsable, la implementación de las medidas de mitigación necesarias y, junto la Jefatura de la Unidad Coordinación Informática y el Encargado de Ciberseguridad, evaluar las acciones realizadas.

8.3 Condiciones consideradas pala la evalaución de la estrategia

El escenario considerado en esta política es la indisponibilidad de los sistemas que soportan los procesos críticos definidos en el alcance del SGSI. Este escenario puede ser provocado por las siguientes causas:

Indisponibilidad de las instalaciones

Corresponde a la pérdida de las instalaciones físicas o suministros básicos que soportan los sistemas de información, frente a la materialización de un desastre, o la imposibilidad de acceder a las instalaciones.

Estas amenazas pueden ser generadas por las siguientes causas:

- Terremoto.
- Fuego.
- Ataques terroristas.
- Interrupciones organizadas o deliberadas (Sabotaje).

Sabotaje de ciberseguridad

De acuerdo a su efecto, los sabotajes de Ciberseguridad se pueden dividir en aquellos:

- Orientados a afectar programas (Software Básico, Aplicaciones o Datos).
- Destinados a afectar las capacidades de procesamiento.
- Con el objetivo de interrumpir las comunicaciones.

Desastres por falla técnica

Pueden dañar seriamente la continuidad de las operaciones tecnológicas, pudiendo afectar a servidores, almacenamiento, las comunicaciones o suministro de energía.

Estas amenazas pueden ser generadas por las siguientes causas:

- Fallos de equipo.
- Fallos en el suministro eléctrico.
- Virus, amenazas y ataques informáticos.

8.4 Requisitos de seguridad

Durante una crisis o desastre, los requisitos de seguridad de la información siguen siendo los mismos existentes en condiciones normales de operación. Es responsabilidad del Encargado de Seguridad de la Información velar por mantener la seguridad de la información durante la administración del evento disruptivo.

Se establecen los siguientes requisitos de seguridad, dependiendo de las circunstancias:

Requisitos de seguridad física:

- Cuidar y proteger áreas que contienen y/o procesan información.
- Proteger y mantener controles físicos de entrada a las áreas seguras.
- Restringir a lo estrictamente necesario el ingreso de proveedores a las áreas seguras, privilegiando a aquellos que sean indispensables para el aseguramiento de la continuidad de la seguridad de la información.
- Verificar las condiciones ambientales de manera de evitar que éstas puedan afectar adversamente a la operación de las instalaciones de procesamiento de información.

Requisitos de seguridad para sistemas y redes:

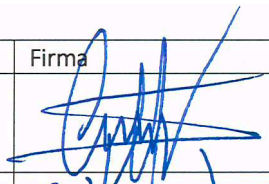
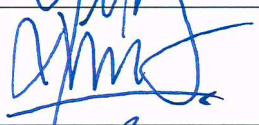
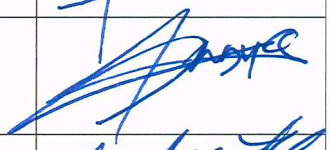
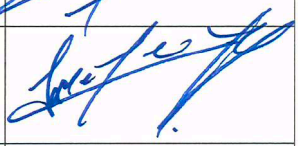
- Si se debe realizar un cambio en los paquetes de software, se deben cumplir todos los requisitos de seguridad descritos en las políticas y procedimientos respecto del desarrollo seguro de software, vigentes en el IND.
- En el caso que la contingencia afecte a las redes, la seguridad de las mismas se debe gestionar siguiendo lo indicado en las políticas y procedimientos para la protección de la información en las redes e instalaciones de procesamiento de información, vigentes en el IND.
- Se debe cautelar el uso seguro de los perfiles de usuario, evitando que la contingencia afecte las reglas de acceso a los distintos sistemas de la Institución.

Para cumplir exitosamente con el objetivo de mantener la seguridad de la información ante la ocurrencia de un evento disruptivo, es necesario involucrar a especialistas de seguridad de la información al establecer, implementar y mantener la continuidad de los procesos de recuperación ante desastres.

8.5 Controles compensatorios

En aquellos casos en que, dadas las condiciones y las contingencias, no es posible mantener los controles de seguridad establecidos, impidiendo el correcto resguardo de la información y los activos de información críticos, el Encargado de Seguridad debe establecer, implementar y mantener controles compensatorios para mantener un nivel aceptable de seguridad de la información, dejando registro de los controles utilizados, la descripción de la contingencia, los controles vulnerados y el impacto de la contingencia en los activos de información afectados.

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración	Cristian Villalobos Zamora	Encargado PMG Seguridad de la Información	
Responsable de Revisión	Edson Maya Vera	Encargado Área de Operaciones	
Responsable de Revisión	Andy Cayuqueo Gonzalez	Encargado Área de Desarrollo	
Responsable de Revisión y Aprobación	Jaime Bustos Brito	Encargado de Ciberseguridad	
Responsable de Revisión y Aprobación	Carola Molina Cecchi	Encargada de Seguridad de la Información	

Control de Cambios

Versión	Fecha	Responsable	Descripción
Versión 1	16-05-2019	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento