1. OBJETIVO

La presente política tiene como propósito responder al nivel necesario de continuidad para la Seguridad de la Información durante situaciones adversas, a fin de evitar interrupciones en los activos críticos del Instituto Nacional de Deportes (IND) como consecuencias de fallas técnicas, desastres naturales o cualquier otro incidente que conlleve una vulneración a la seguridad de la información o afecte el normal funcionamiento del IND.

2. ALCANCE

Esta Política abarca todo el dominio de la Administración de Incidentes de Seguridad de la Información de la NCh-ISO 27001:2013, aplicando para todo el personal que trabaje en, o para el IND, ya sean funcionarios de planta, contrata, honorarios, regidos por el Código del Trabajo, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios para el IND, cuyas funciones dan soporte a los procesos de provisión vigentes, de acuerdo a lo establecido en la Ficha de Definiciones Estratégicas (A1).

3. DOCUMENTOS RELACIONADOS

- Norma NCh-ISO 27002:2013; control A.16.01.01; A.16.01.02; A.16.01.03; A.16.01.04; A.16.01.05; A.16.01.06; A.16.01.07.
- Decreto Supremo N° 83, del 12-01-2005, Articulo 35.
- Política General de Seguridad de la Información.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.

4. DEFINICIONES

Activos de Información: corresponde a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
De esta forma se pueden distinguir 3 niveles básicos de activos de información:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
- Los Equipos, Sistemas de Información, Infraestructura que soportan esta información.
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Amenaza: es un evento con el potencial de afectar negativamente la Confidencialidad, Integridad y/o disponibilidad de los Activos de Información de una organización.

Evento de Seguridad: se considera un evento de seguridad la ocurrencia de una situación que indica una posible violación a las políticas de seguridad o fallas en los controles que no genere un impacto en el desarrollo de las operaciones de la organización y que puede ser controlado rápidamente.

Incidente de Seguridad: cualquier evento o situación que comprometa de manera IMPORTANTE la disponibilidad, integridad y/o confidencialidad de los activos de información, junto con la plataforma tecnológica, procesos y aplicativos que permitan acceder a ésta en forma oportuna. También se entiende como incidente de seguridad la violación de una política, estándar o procedimiento de seguridad de la información.

Ejemplos de incidentes de seguridad de la información:

- Pérdida de servicio, de equipos o de instalaciones;
- Mal funcionamiento o sobrecargas del sistema;
- Errores humanos;
- No cumplimiento con políticas o procedimientos;
- Violaciones de las disposiciones de seguridad física;
- Mal funcionamiento de software o hardware;
- Violaciones de acceso.

Los incidentes obedecen a la siguiente clasificación:

- Denegación de servicios computacionales.
- Código malicioso.
- Accesos no autorizados.
- Mal uso de recursos.
- Aplicativos de negocios.
- Violación de normativa de seguridad, código de ética y reglamento interno.

Debilidad: Cualquier evento o circunstancia que pudiera dar origen a un incidente de seguridad, a causa de la existencia de un riesgo no detectado o por la ineficacia o ausencia de control de seguridad de la información.

5. ROLES Y RESPONSABILIDADES

- Comité de Seguridad de la Información:
  - Supervisar la implementación de las actividades que se desprenden de la presente política.
  - Tomar la decisión de activar planes de contingencia antes incidentes que afecten gravemente a la continuidad de los procesos de la institución.

- Encargado/a de Seguridad de la Información:
  - Velar por el correcto cumplimiento de esta política.
  - Monitorear el avance general de las estrategias de control que se desprenden de la presente política.
  - Gestionar el proceso de respuesta ante incidentes de seguridad de la información, los planes de acción y el aprendizaje de los mismos.

- Área de Operaciones:
  - Punto de Contacto, el cual debe derivar el incidente o debilidad reportados al área de que corresponda para su tratamiento.

- Dirección Instituto Nacional de Deportes
  - Disponer los recursos necesarios a fin de brindar una apropiada gestión de los incidentes de Seguridad de la Información, mediante la implementación de procedimientos para la gestión de incidentes de seguridad de la información.

- Personal IND:
  - Dar cumplimiento a la presente Política, independiente del cargo que desempeñe y de su situación contractual.
  - Reportar los incidentes y/o debilidades de seguridad que detecte, utilizando los canales dispuestos para tal efecto.

6. DIFUSIÓN

La forma de difusión de la presente Política será a través de su publicación en la sección “Seguridad de la Información” de la intranet institucional una vez que sea formalizada.

7. REVISIÓN Y EVALUACIÓN

La presente Política se debe revisar y evaluar su correcta aplicación cuando se cumpla un año de su aprobación y formalización o cada vez que se detecte un evento que propicie un ajuste de las declaraciones establecidas; en ambos casos; estas revisiones y evaluaciones se realizarán en sesiones del Comité de Seguridad de la Información.

8. IDENTIFICACIÓN DE AMENAZAS

ACTIVO	AMENAZA
Entorno	▪ Desastres Naturales ▪ Incendio
Equipamiento	▪ Desastres Naturales ▪ Incendio ▪ Fallas de hardware ▪ Fallas de servicio ▪ Hurto
Sistema de Información	▪ Hurto de código fuente ▪ Accesos no autorizados ▪ Falla de hardware ▪ Código malicioso
Información	▪ Hurto ▪ Alteración ▪ Divulgación no autorizada ▪ Destrucción
Recursos Humanos	▪ Desastres naturales ▪ Incendio ▪ Enfermedades ▪ Huelgas ▪ Ingeniería Social

9. CATEGORIZACIÓN DE LOS INCIDENTES

- **Incidentes Críticos:** estos incidentes pueden afectar la integridad o la confidencialidad de la información, lo cual tiene como resultado la pérdida directa del activo:
  - El incidente requiere solución inmediata, ya que éste causa la completa pérdida de un servicio o la interrupción de las actividades laborales.
  - Se genera un impacto crítico en el cliente.
  - Se genera un impacto crítico en aplicaciones o procesos de negocio.

    - Afecta a un grupo de usuarios o a un usuario de servicios informáticos de alto rango.
- Incidentes Severos: estos incidentes afectan típicamente la disponibilidad de la información, pero no la integridad de la misma:
    - La plataforma informática, sistema de información o aplicación que opera con procesos críticos.
    - La plataforma informática, sistema de información o aplicación no está operativo, pero no requiere una solución inmediata.
    - El impacto no es crítico.
- Incidentes Normales: estos incidentes pueden afectar la confidencialidad, integridad o disponibilidad de la información, sin embargo no existe pérdida alguna:
    - La plataforma informática, sistema de información o aplicación opera con funcionalidades limitadas.
    - La plataforma informática, sistema de información o aplicación no está operativo, pero existen alternativas paralelas y están disponibles.
    - No se ven afectados los sistemas de información importante para el negocio.
- Incidentes Menores: estos incidentes no afectan la seguridad de la información ni de las telecomunicaciones:
    - Se acuerda y programa con el usuario de servicios informático la atención, para una fecha acordada. En este tipo de soporte se incluyen:
    - Actualizaciones de hardware y software.
    - Movimientos de oficinas o reasignación de equipos.
    - Reporte y registro de fallas de hardware y software.

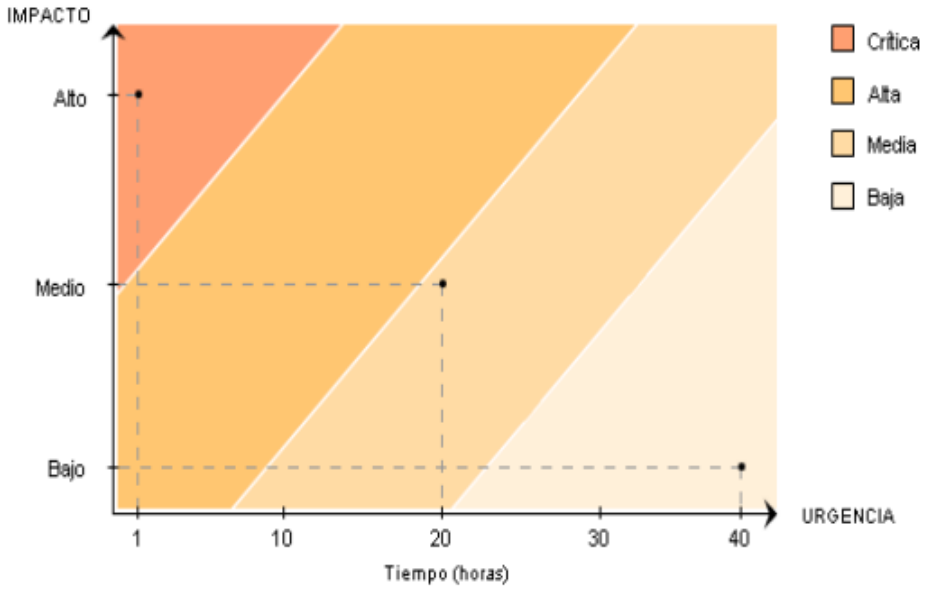
Es normal que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

El nivel de prioridad se basará esencialmente en dos parámetros:

- Impacto: determinara la importancia del incidente dependiendo de cómo éste afecta los procesos de la institución y/o el número de usuarios afectados:
    - Bajo: no interrumpe los procesos generales de la institución y afecta solo a 1 usuario.
    - Medio: interrumpe momentáneamente los procesos de la institución y afecta a más de un usuario, pero a menos de cinco.
    - Alto: interrumpe seriamente los procesos de la institución y afecta a más de 5 funcionarios.

- Urgencia: dependerá del tiempo máximo de demora que pueda aceptar el/la usuario/a para la resolución del incidente. A la aceptación de más tiempo de espera, significará que el incidente s menos urgente.

Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente. El siguiente diagrama nos muestra un diagrama de prioridades en función de la urgencia e impacto del incidente:



10. POLÍTICA

La presente Política de Gestión de Incidentes de Seguridad de la Información se integrará a la normativa del Instituto Nacional de Deportes, incluyendo su difusión previa, así como de los documentos relacionados a esta.

10.1 Informe de Incidentes de Seguridad de la Información

Los incidentes de Seguridad de la información se deben informar al *Punto de Contacto* lo más rápido posible a través de canales de comunicación y administración formales.

Canales de información:

1) Sistema de Gestión de Incidentes "Mantis".
2) De forma telefónica:
    a. Anexo 1278
    b. Anexo 1279
    c. Anexo 1288
3) Correo electrónico: incidentes@ind.cl
4) De forma presencial el/la Encargado/a de Seguridad. Piso 4 Depto. Informática.

Algunas de las situaciones que se deberían considerar para el reporte de incidentes de seguridad incluyen:

a) Controles de seguridad ineficaces.
b) Vulnerabilidad en la integridad, la confidencialidad o a las expectativas de disponibilidad de la información.
c) Incumplimientos en las Políticas de seguridad.
d) Incumplimiento en las disposiciones de seguridad física.
e) Cambios no controlados a los sistemas de información.
f) Fallas en el software y/o hardware.
g) Violaciones de accesos tanto físicos como a los sistemas de información.
h) Ataques de código malicioso.

Ante la detección de un evento o incidente de seguridad, el/la Encargado/a de Seguridad de la información del IND deberá ser informado tan pronto como sea posible. Este supervisará las acciones necesarias para la resolución del incidente. Asimismo, mantendrá al resto del Comité de Seguridad de la Información al tanto del desarrollo de las actividades.

10.2 Evaluación y decisión sobre los incidentes de Seguridad de la Información

El Punto de Contacto deberá evaluar el evento de seguridad de la información utilizando la escala de clasificación de eventos e incidentes de seguridad de la información y decidir si el evento se debería clasificar como un incidente de seguridad de la información. La clasificación y la priorización de incidentes pueden ayudar a identificar el impacto y el alcance de un incidente.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- Categorización
- Nivel de prioridad

- Monitoreo del estado y tiempo de respuesta esperado.

Se deben registrar los resultados de la evaluación y la decisión en detalle con fines de referencia y verificaciones futuras.

10.3 Respuesta ante incidentes de Seguridad de la Información

El Punto de Contacto y otras áreas pertinentes del IND deben responder ante los incidentes de Seguridad de la Información.

La respuesta debería incluir lo siguiente:

a) Recopilar la evidencia lo más pronto posible después de la ocurrencia.
b) Escalamiento, según sea necesario.
c) Asegurarse de que todas las actividades de respuesta se registren correctamente para el posterior análisis.
d) Comunicación de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a otras personas u organizaciones internas o externas con una necesidad de conocimiento.
e) Manejar las debilidades de la seguridad de la información que causan o contribuyen al incidente.
f) Una vez que se ha manejado el incidente correctamente, se debería cerrar y registrar formalmente.
g) Se debe realizar un análisis post-incidente, según sea necesario, para identificar el origen del incidente.

Mayor detalle de la respuesta ante incidente, se encuentra en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

10.4 Aprendiendo de los incidentes de seguridad de la información

Se debe utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.

La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de contar con controles mejorados o adicionales para limitar la frecuencia, el daño y el costo de las ocurrencias futuras o bien se deben considerar en el proceso de revisión de las políticas de seguridad.

10.5 Recolección de evidencia

Se deben definir y aplicar procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir para propósitos de acciones legales y disciplinarias.

Cuando se siga el proceso disciplinario interno, la evidencia debe ser clara y suficiente para comprobar las acciones, para ello se deberá:

- Registrar información que rodea a la evidencia.
- Tomar fotografías del entorno de la evidencia (si aplica).
- Registrar la evidencia.
- Rotular todos los medios que serán tomados como evidencia.
- Almacenar toda la evidencia en forma segura.
- Generar copias de seguridad de la evidencia original.

Cuando la acción involucre la ley, ya sea penal o civil, la evidencia presentada debe ser conformada y aterrizada según las leyes correspondientes y ante la autoridad correspondiente y se deberá velar por la calidad e integridad de ésta.

Cualquier incumplimiento de políticas o procedimientos asociados a las materias enumeradas a continuación, podrían generar un incidente de seguridad que amerite una investigación y su correspondiente sanción disciplinaria o legal, según corresponda a la naturaleza y gravedad del incidente.

- Fuga o uso indebido de información.
- Violaciones de accesos tanto físicos como a los sistemas de información.
- Cambios no autorizados a la infraestructura tecnológica de la institución.
- Pérdida o robo de equipos y medios móviles.
- Vulneraciones a los controles de uso de recursos de internet.
- Vulneración a los controles de uso de equipos personales e instalación o uso ilegal de software.
- Uso indebido del correo electrónico institucional.
- Incumplimiento de políticas de cuentas de usuarios y contraseña.

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 y Aprobación	Carola Molina Cecchi	Encargada de Seguridad de la Información	

Control de Cambios

Versión	Fecha	Responsable	Descripción
Versión 1	18-07-2017	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento para dar cumplimiento al PMG-SSI 2017 y abordar requerimientos internos del IND.
Versión 2	10-07-2018	Cristian Villalobos Z.	Se modifica la difusión de la política, se detalla la definición de incidente y se ajustan las responsabilidades.
Versión 3	16-05-2019	Cristian Villalobos Z.	Se incluye la opción de reportar los incidentes a través de la plataforma Mantis.