RESOLUCIÓN EXENTA

Nº: 03050/2021

MAT.: APRUEBA PROCEDIMIENTO DENOMINADO "IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"

Santiago, 27/ 12/ 2021

VISTOS:

1. La Ley N°19.712, del Deporte;

2. La Ley N°18.575 Orgánica Constitucional sobre Bases Generales de la Administración del Estado;

3. La Ley N°19.880 que establece las Bases de los Procedimientos Administrativos que rigen los actos de los

4. El Decreto Supremo N°23, de 13 de agosto de 2020, del Ministerio del Deporte, que nombra en el cargo a la Directora Nacional del Instituto Nacional de Deportes de Chile;

5. La Resolución Exenta N°3083, de 2018, del IND.

6. La Resolución Exenta N°4239 del 30 de diciembre de 2019, que "Aprueba Matriz de Plan de Mejoras correspondiente al convenio de colaboración entre el Instituto Nacional de Deportes de Chile y la Contraloría General de la República, por el Programa de Apoyo al Cumplimiento", del Instituto Nacional de Deportes de Chile.

CONSIDERANDO:

1. Que, el Instituto Nacional de Deportes de Chile es un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, al que le corresponde ejecutar la política nacional de deportes y tiene a su cargo la promoción de la cultura deportiva en la población, la asignación de recursos para el desarrollo del deporte y la supervigilancia de las organizaciones deportivas en los términos establecidos por la Ley N°19.712, de Deportes.

2. Que para la organización interna del Servicio resulta del todo necesario establecer normas procedimentales para el desarrollo de las tareas que la ley ha dispuesto para este Servicio.

3. Que, el procedimiento cuyo texto se aprueba en este acto, establece de manera detallada, ordenada y sistemática, las actividades asociadas a los subprocesos que realiza el Comité de Seguridad de la Información (CSI), para el adecuado funcionamiento, seguimiento y evaluación del Sistema de Gestión de Seguridad de Información (SGSI), de acuerdo a la normativa vigente.

RESUELVO:

1. APRUÉBASE Procedimiento denominado "Implementación del sistema de gestión de seguridad de la información", cuyo tenor se detalla en el documento anexo.

2. PUBLÍQUESE, la presente Resolución Exenta, en el banner de gobierno transparente del Instituto Nacional de Deportes de Chile.

ANOTESE, COMUNIQUESE Y ARCHIVESE

ESTE DOCUMENTO CUENTA CON FIRMA ELECTRÓNICA AVANZADA
IND Instituto Nacional de Deportes

ISRAEL FERNANDO CASTRO LOPEZ
DIRECTOR NACIONAL (S)

INSTITUTO NACIONAL DE DEPORTES DE CHILE

SPO/JVR/ICL/KAA/APV/CMC/CVZ

Anexos

Nombre	Tipo	Archivo	Copias	Hojas
Procedimiento SSI	Digital	Ver		

Distribución:
DIVISION DE ADMINISTRACION Y FINANZAS
DEPARTAMENTO INFORMATICA
UNIDAD DE PLANIFICACION Y CONTROL DE GESTION
UNIDAD DE AUDITORIA INTERNA

PROCEDIMIENTO

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN INSTITUCIONAL

Comité de Seguridad de la Información.
Instituto Nacional de Deportes (IND).

Control de Cambios.

Versión Nº	Fecha	Responsable Elab. / Modif.	Responsable Aprobación	Alcance y/o motivo de la revisión
1		Cristian Villalobos Z.		Se elabora la primera versión del documento.

Tabla de Contenidos

1. Objetivo.

El objetivo del presente documento es describir de manera detallada, ordenada y sistemática, las actividades asociadas a los subprocesos que realiza el Comité de Seguridad de la Información (CSI), para el adecuado funcionamiento, seguimiento y evaluación del Sistema de Gestión de Seguridad de Información (SGSI), de acuerdo a la normativa vigente.

La información presentada facilita la estandarización de tareas, la delimitación de responsabilidades y funciones, la toma de decisiones y la identificación de oportunidades de mejora, impactando de manera positiva en la gestión interna de la institución.

2. Alcance.

El procedimiento da cuenta de los 5 subprocesos que realiza el Comité de Seguridad de la Información para implementar y gestionar efectivamente el Sistema de Gestión de Seguridad de la Información institucional. A continuación, se detalla cada uno de ellos, con su respectiva actividad de inicio y término.

1. **Subproceso 1 "Revisión de la Política General de Seguridad de la Información institucional":** inicia con el envío, por parte del/la Encargado/a de Seguridad de la Información (ESI), de la Política General de Seguridad de la Información (PGSI) institucional vigente al Comité de Seguridad de la Información (CSI) para su revisión y finaliza con el respaldo de la PGSI y su resolución, si corresponde, en la carpeta compartida de uso institucional.
2. **Subproceso 2 "Aprobación de Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información Institucional":** inicia con la planificación y definición, por parte del/la ESI, de las Políticas, Planes y/o Procedimientos a ser revisados durante el año en curso y finaliza con el respaldo, en la carpeta compartida de uso institucional, de la documentación en su versión final.
3. **Subproceso 3 "Gestión de riesgos asociados a los activos de información de los procesos institucionales":** Se subdivide en 2 etapas, correspondientes a (1) Formulación del Plan de Tratamiento de Seguridad de la Información año t+1 y (2) Monitoreo del Plan de Tratamiento de Seguridad de la Información año t-1. La Etapa 1 comienza con el levantamiento, por parte del ESI, de los activos de información para el año t y finaliza con el respaldo del Plan de Tratamiento de SI año t+1 aprobado, en la carpeta compartida de uso institucional. La Etapa 2 comprende desde la elaboración de la minuta con el estado de avance del Plan de Tratamiento de SI año t-1, por parte del ESI, hasta la respuesta a las observaciones del Comité de Riesgos, si corresponde.
4. **Subproceso 4 "Monitoreo y Evaluación del Sistema de Gestión de Seguridad de la Información institucional"**: inicia con la elaboración de del Reporte de Alertas e Incidentes mes t, realizado por el ESI, y finaliza con el respaldo, en la carpeta compartida de uso institucional, de toda la documentación asociada a la etapa.

3. Referencias.

- Decreto Supremo N°83, 12 de enero 2005. Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos.
- Resolución Exenta N°3369, 29 de octubre 2018. Aprueba Nueva Composición y Normativa del Comité de Seguridad de la Información del Instituto Nacional de Deportes.
- Resolución Exenta N°2760, 30 de agosto 2019. Aprueba Política General de Seguridad de la Información del Instituto Nacional de Deportes.

- Resolución Exenta N°1738, 28 de agosto 2020. Designa Encargado de Seguridad de la Información en el Instituto Nacional de Deportes.
- Norma NCh-27001:2013.
- Instructivo Presidencial N°8, 23 de octubre 2018. Imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos en los órganos de la Administración del Estado.
- Política de Cumplimiento Sistema de Seguridad de la Información, 16 de mayo 2019.
- Política de Administración de Activos de Información, 15 de mayo 2019, versión 2.

4. Definiciones.

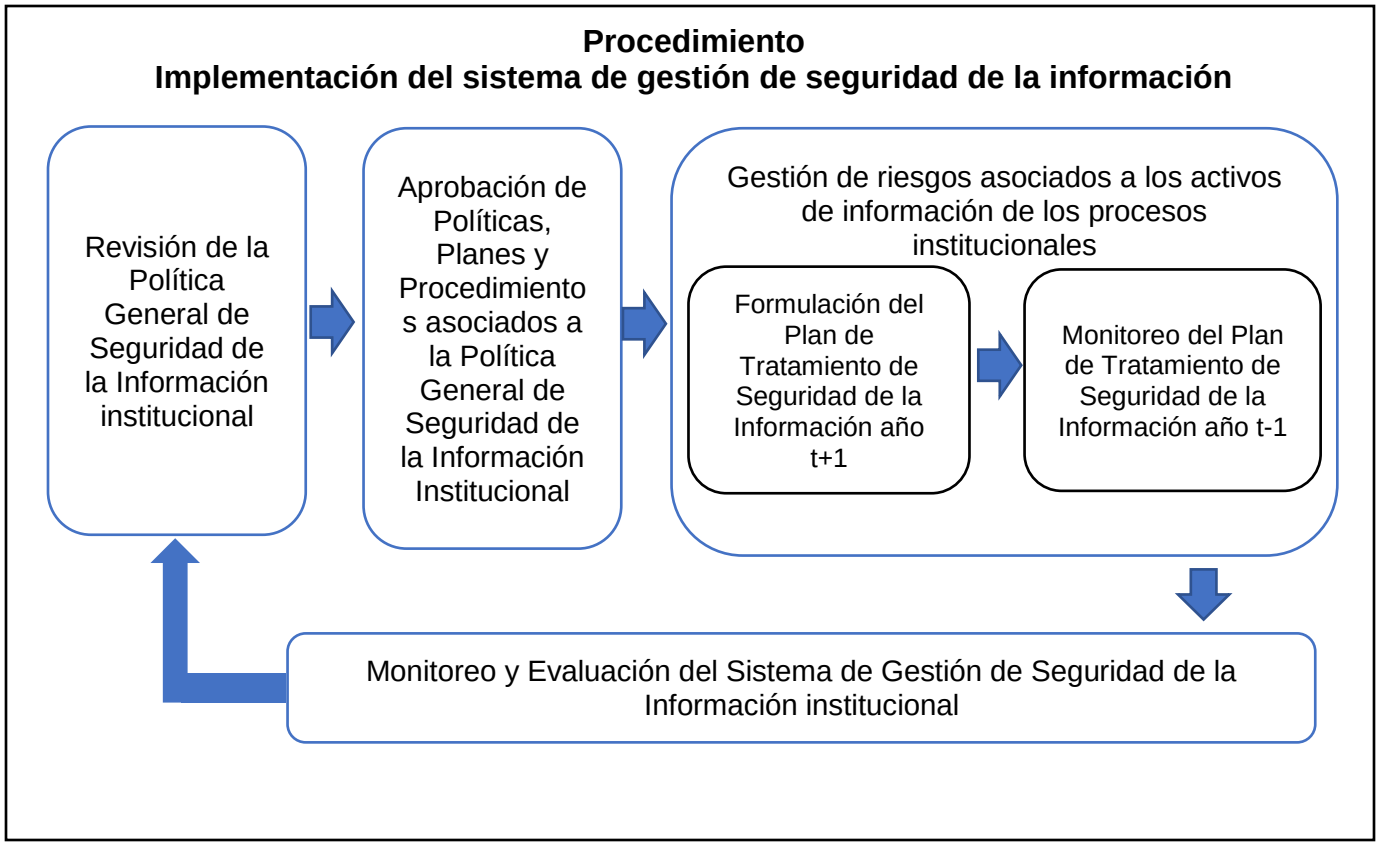
Sistema de Gestión de Seguridad de la Información (SGSI).	Es el diseño, implementación, mantención de y mejora continua de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
Política General de Seguridad de la Información (PGSI).	Es un documento, normativo institucional, orientado a proteger la información en la totalidad de su ciclo de vida (creación, difusión, modificación, almacenamiento, preservación y eliminación), los medios que permiten dicho ciclo y las personas que acceden y/o manipulan la información; lo anterior, con el fin de garantizar su integridad, disponibilidad y confidencialidad.
Seguridad de la Información.	Son todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger los activos de información de la organización y sus usuarios en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
Ciberseguridad.	Es el conjunto de herramientas, políticas, métodos de gestión, prácticas y tecnologías que pueden utilizarse para proteger los activos de información de la organización y sus usuarios en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
Comité de Seguridad de la Información (CSI).	Integrado por el/la Encargado/a de Seguridad, quien lo presidirá, la Jefatura del Departamento Jurídico, Jefatura de la División de Administración y Finanzas, Unidad de Planificación y Control de Gestión y Encargado PMG de Sistema de Seguridad de la Información. Su objetivo es Gestionar la Política de Seguridad de la Información de la Institución.

Encargado de Seguridad de la Información (ESI)	Funcionario/a que cumple la función de supervisar el cumplimiento de la normativa, asesorar en materias de Seguridad de la Información a la Alta Dirección y a los funcionarios del IND que así lo requieran.
Encargado de Ciberseguridad (ECS)	Funcionario/a responsable de la seguridad informática del IND.
Alta Dirección	Compuesta por el/la Director/a Nacional, Directores/as Regionales y las Jefaturas de la División de Administración y Finanzas, División de Infraestructura y Recintos, y División de Actividad Física y Deportes.
Activo de información crítico	Son todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
Incidente	Está indicado por uno o múltiples eventos no esperados. Esto tiene una alta probabilidad de comprometer la continuidad de las operaciones del negocio. Se puede definir como un incidente de seguridad de la información al acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de activos de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Normativa de Seguridad de la Información del Servicio.

5. Formularios / Formatos Aplicables.

- Reporte de Alertas e Incidentes.
- Informe Anual de Resultados SGSI.

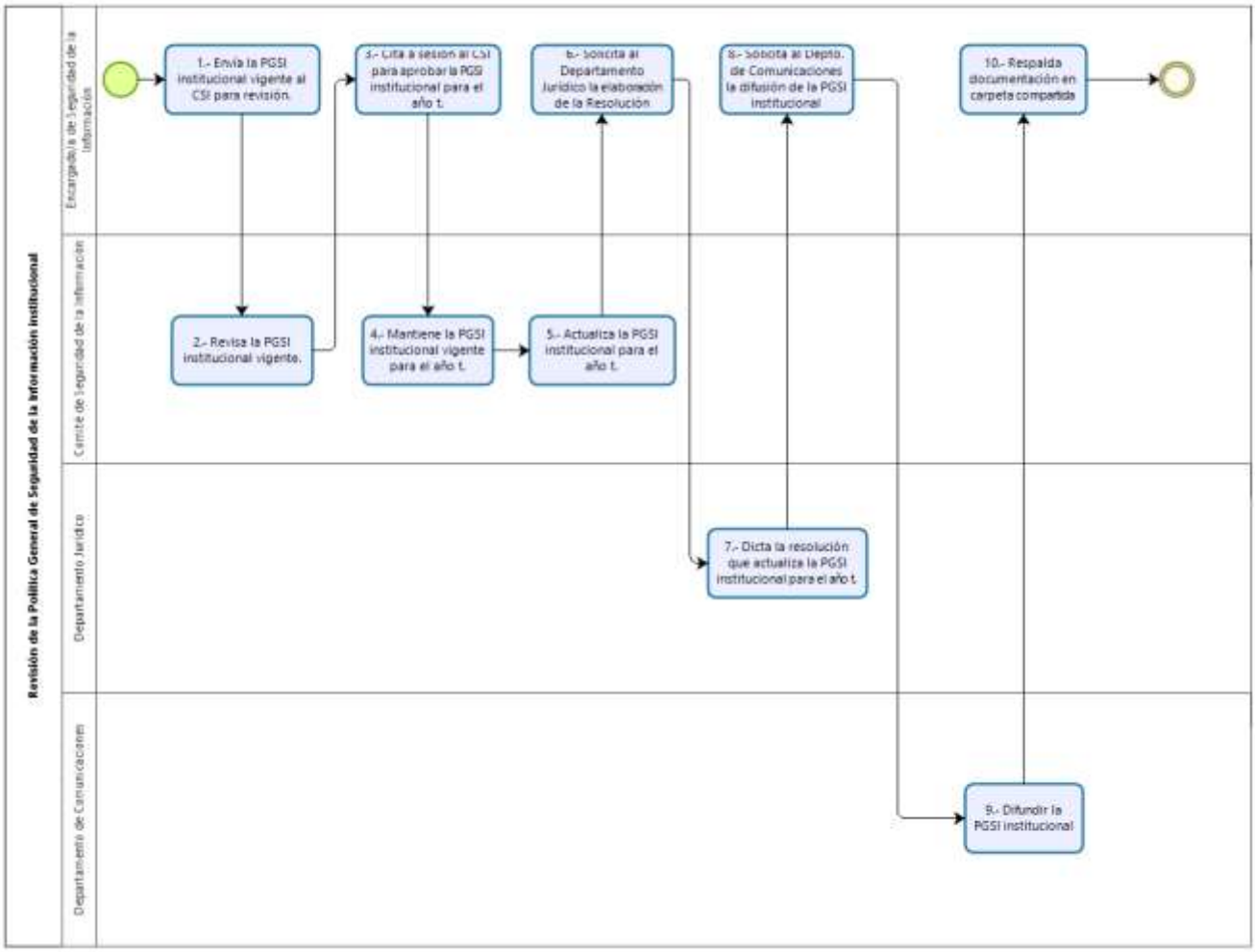
6. Modo de Operación:



6.1. Subproceso 1: Revisión de la Política General de Seguridad de la Información institucional.

Objetivo: Revisar la Política General de Seguridad de la Información institucional vigente y proponer a la Jefatura Superior del Servicio, si corresponde, su actualización, con el fin de asegurar su continuidad, idoneidad, eficiencia y efectividad.

6.1.1. Flujograma del Subproceso 1: Revisión de la Política General de Seguridad de la Información institucional.



6.1.2. Matriz del Subproceso 1: Revisión de la Política General de Seguridad de la Información institucional.

N°	¿Quién?	¿Qué?	¿Cuándo?	¿Cómo?	Registro
1	Encargado/a de Seguridad de la Información	Envía la PGSI institucional vigente al CSI para revisión.	Segundo trimestre del año en curso	A través de correo electrónico, envía la PGSI institucional vigente a los integrantes del CSI y otorga un plazo aproximado de 2 semanas para revisar y evaluar la pertinencia de su actualización.	Correo electrónico.
2	Comité de Seguridad de la Información	Revisa la PGSI institucional vigente.	Segundo trimestre del año en curso	Recibe y revisa la Política General de Seguridad de Información institucional vigente. Para evaluar su actualización, considera lo siguiente: - Ocurrencia de eventos o cambios significativos en tecnología, personal, presupuesto u otro, que impacten directamente la PGSI institucional. - Informe Anual de Resultados SGSI año t-1. - Solicitudes de modificación por parte de otra Área de la Institución o por el/la Directora/a Nacional.	Correo electrónico.
3	Encargado/a de Seguridad de la Información	Cita a sesión al CSI para aprobar la PGSI institucional para el año t.	Segundo trimestre del año en curso	A través de correo electrónico, cita a los miembros del CSI a sesionar para definir si se mantiene la PGSI institucional vigente o se actualiza, en base a las observaciones levantadas durante la revisión. Esta sesión puede realizarse de manera online, presencial, y/o a través de coordinación mediante correo electrónico, cuando la optimización del tiempo así lo amerite.	Correo electrónico.

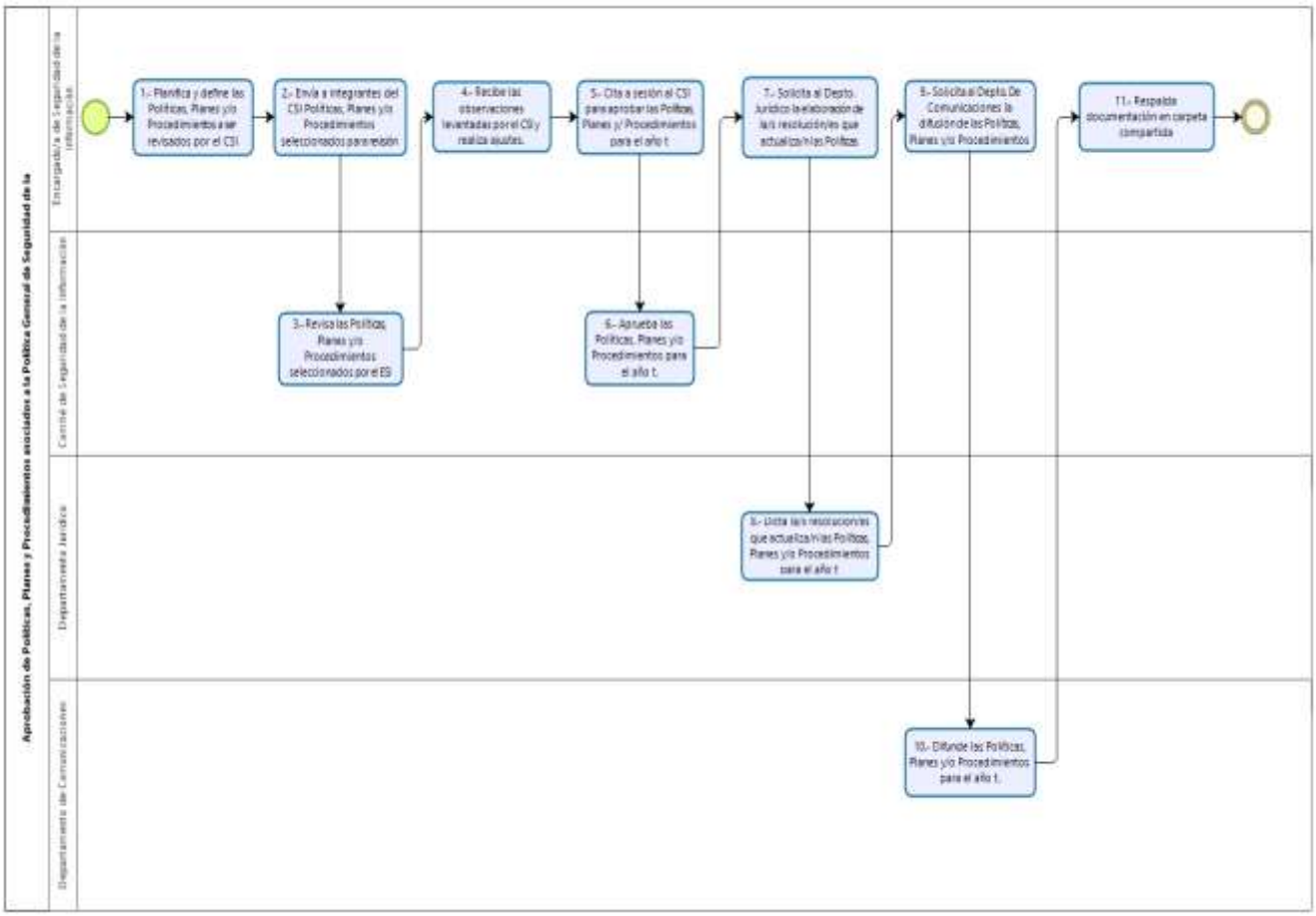
4	Comité de Seguridad de la Información	Mantiene la PGSI institucional vigente para el año t.	Segundo trimestre del año en curso.	En consideración a la evaluación realizada en conjunto con el ESI, mantiene la Política General de Seguridad de la Información institucional vigente para el año t.	Acta de sesión CSI.
5	Comité de Seguridad de la Información	Actualiza la PGSI institucional para el año t.	Segundo trimestre del año en curso.	En consideración a la evaluación realizada, actualiza la Política General de Seguridad de la Información institucional para el año t.	Acta de sesión CSI.
6	Encargado/a de Seguridad de la Información	Solicita al Departamento Jurídico la elaboración de la Resolución	Segundo trimestre del año en curso.	Solicita al Departamento Jurídico, mediante Plataforma Cero Papel. Gestión Documental, la elaboración de la resolución correspondiente.	Sistema de Gestión Documental.
7	Departamento Jurídico	Dicta la resolución que actualiza la PGSI institucional para el año t.	Segundo trimestre del año en curso.	Gestiona la firma del/la Director/a Nacional y dicta la resolución que actualiza la PGSI institucional para el año t. Envía la resolución completamente tramitada al ESI, a través del Sistema de Gestión Documental.	Resolución tramitada. Sistema de Gestión Documental.
8	Encargado/a de Seguridad de la Información	Solicita al Depto. de Comunicaciones la difusión de la PGSI institucional	Segundo trimestre del año en curso.	Solicita al Departamento de Comunicaciones la elaboración de mailings, boletines u otro/s para difundir la Política General de Seguridad de la Información institucional.	Correo electrónico.
9	Departamento de Comunicaciones	Difundir la PGSI institucional	Segundo trimestre del año en curso.	Envía mailings, boletines u otro/s a todos los/las funcionarios/as de la Institución con la Política General de Seguridad de la Información institucional.	Correo electrónico

10	Encargado/a de Seguridad de la Información	Respalda documentación en carpeta compartida	Segundo trimestre del año en curso.	Guarda en carpeta compartida de uso institucional, la versión final de la Política General de Seguridad de la Información y la resolución que aprueba su actualización, si corresponde.	Carpeta compartida.

6.2. Subproceso 2: Aprobación de Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información Institucional.

Objetivo: Revisar las Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información institucional y aprobar las versiones vigentes o actualizadas para el año en curso.

6.2.1. Flujograma Subproceso 2: Aprobación de Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información institucional.



6.2.2. Matriz Subproceso 2: Aprobación de Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información institucional.

N°	¿Quién?	¿Qué?	¿Cuándo?	¿Cómo?	Registro
1	Encargado/a de Seguridad de la Información	Planifica y define las Políticas, Planes y/o Procedimientos a ser revisados por el CSI.	Meses de junio, septiembre y diciembre del año en curso.	Revisa la documentación y normativa asociada a la Política General de Seguridad de la Información institucional y selecciona al menos 5 Políticas, Planes y/o Procedimientos para ser evaluados por el CSI. La selección considera lo siguiente: - Políticas, Planes y/o Procedimientos cuya revisión se encuentre pendiente del/los años/s anterior/es. - Política General de Seguridad de la Información Institucional y su actualización, si corresponde. - Cambios en la normativa vigente, tecnológicos, presupuestarios, de recursos humanos, etc. que impacten al SGSI.	Plan de revisión año t.
2	Encargado/a de Seguridad de la Información	Envía a integrantes del CSI Políticas, Planes y/o Procedimientos seleccionados para revisión.	Meses de junio, septiembre y diciembre del año en curso.	Envía la documentación seleccionada a través de correo electrónico a los integrantes del CSI y otorga un plazo aproximado de 2 semanas para revisión y ajustes, si corresponde.	Correo electrónico.
3	Comité de Seguridad de la Información	Revisa las Políticas, Planes y/o Procedimientos seleccionados por el ESI.	Meses de junio, septiembre y diciembre del año en curso.	Recibe y revisa la documentación seleccionada por el ESI. Si lo estima pertinente, emite observaciones y/o incorpora ajustes. Estas observaciones son enviadas al ESI a través de correo electrónico.	Correo electrónico.

4	Encargado/a de Seguridad de la Información	Recibe las observaciones levantadas por el CSI y realiza ajustes.	Meses de junio, septiembre y diciembre del año en curso.	Recibe las observaciones y/o comentarios realizados por el CSI y ajusta las Políticas, Planes y/o Procedimientos, si corresponde.	Correo electrónico.
5	Encargado/a de Seguridad de la Información	Cita a sesión al CSI para aprobar las Políticas, Planes y/ Procedimientos para el año t.	Meses de junio, septiembre y diciembre del año en curso.	A través de correo electrónico, cita a los miembros del CSI a sesionar para definir si se mantienen las versiones vigentes de las Políticas, Planes y/o Procedimientos o se actualizan en base a las observaciones levantadas durante la revisión. Esta sesión puede realizarse de manera online, presencial y/o a través de coordinación mediante correo electrónico, cuando la optimización del tiempo así lo amerite.	Correo electrónico.
6	Comité Seguridad de la Información	Aprueba las Políticas, Planes y/o Procedimientos para el año t.	Meses de junio, septiembre y diciembre del año en curso.	En conjunto con el ESI, revisa la documentación y aprueba las versiones vigentes o actualizadas de las Políticas, Planes y/o Procedimientos para el año t.	Acta de sesión CSI.
7	Encargado/a de Seguridad de la Información	Solicita al Departamento Jurídico la elaboración de la/s resolución/es que actualiza/n las Políticas, Planes y/o Procedimientos para el año t.	Meses de junio, septiembre y diciembre del año en curso.	Para aquellas Políticas, Planes y/o Procedimientos que fueron actualizados, se solicita al Departamento Jurídico, mediante el Sistema de Gestión Documental, la elaboración de la/s resolución/es correspondientes.	Sistema de Gestión Documental.

8	Departamento Jurídico	Dicta la/s resolución/es que actualiza/n las Políticas, Planes y/o Procedimientos para el año t.	Meses de junio, septiembre y diciembre del año en curso.	Gestiona la firma del/la Director/a Nacional y dicta la/s resolución/es que actualiza/n las Políticas, Planes y/o Procedimientos para el año t. Envía la/s resolución/es completamente tramitadas al ESI, a través del Sistema de Gestión Documental.	Resolución/es tramitadas. Sistema de Gestión Documental.
9	Encargado/a de Seguridad de la Información	Solicita al Depto. De Comunicaciones la difusión de las Políticas, Planes y/o Procedimientos	Meses de junio, septiembre y diciembre del año en curso.	Solicita al Departamento de Comunicaciones la elaboración de mailings, boletines u otro/s para difundir las Políticas, Planes y/o Procedimientos para el año t.	Correo electrónico
10	Departamento de Comunicaciones	Difunde las Políticas, Planes y/o Procedimientos para el año t.	Meses de junio, septiembre y diciembre del año en curso.	Envía mailings, boletines u otros a todos los/las funcionarios/as de la Institución con las Políticas, Planes y/o Procedimientos para el año t.	Correo electrónico
11	Encargado/a de Seguridad de la Información	Respalda documentación en carpeta compartida	Meses de junio, septiembre y diciembre del año en curso.	Guarda en carpeta compartida de uso institucional, las versiones finales de las Políticas, Planes y/o Procedimientos y las resoluciones respectivas, si corresponde.	Carpeta compartida

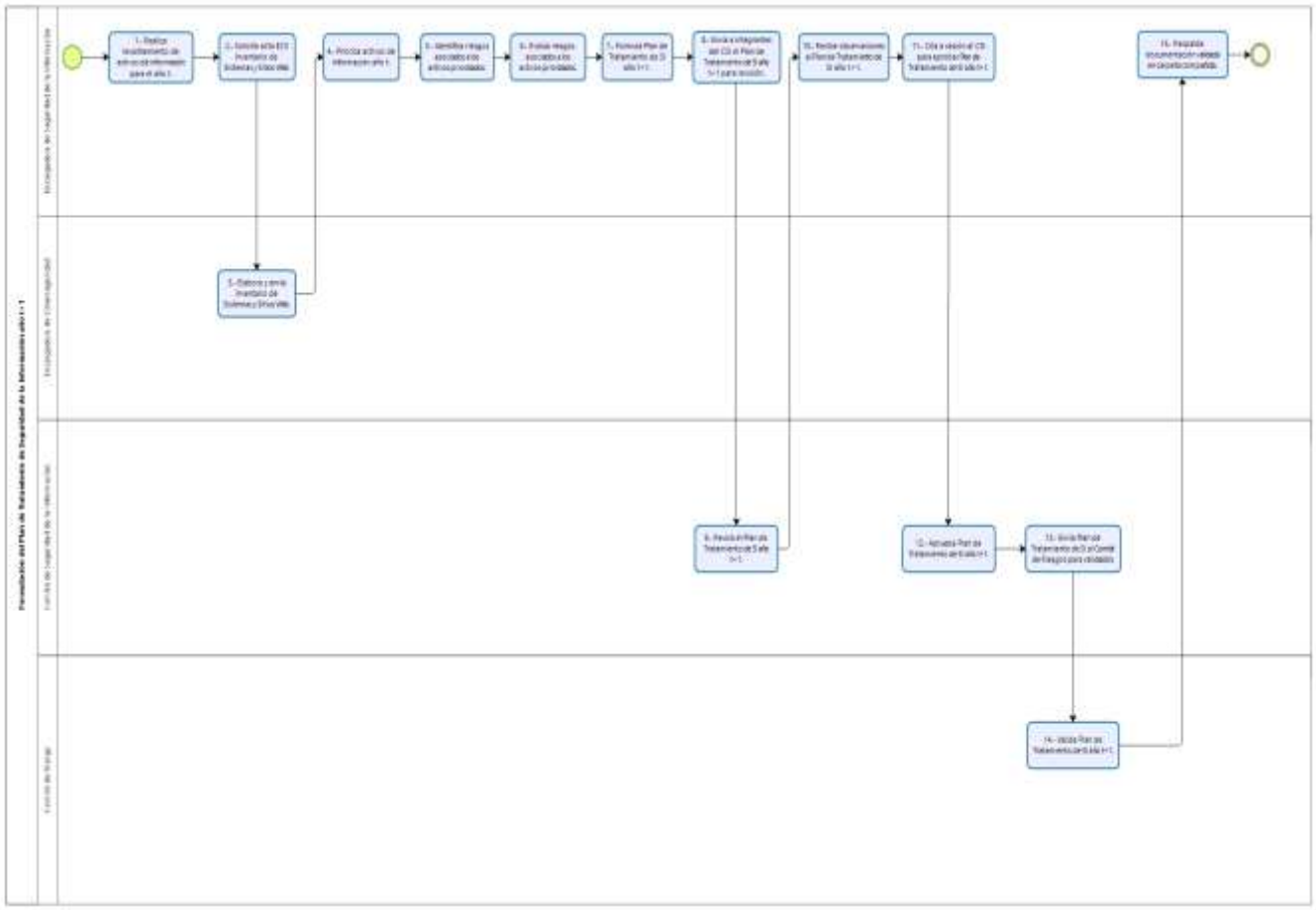
6.3. Subproceso 3: Gestión de riesgos asociados a los activos de información de los procesos institucionales.

Objetivo: Gestionar los riesgos de Seguridad de la Información de los activos vinculados con los procesos de provisión de productos estratégicos (bienes y servicios), asegurando la continuidad de los servicios críticos de la Institución para lograr conservar la confidencialidad, integridad y disponibilidad de la información.

6.3.1. Etapa 1: Formulación del Plan de Tratamiento de Seguridad de la Información año t+1.

Objetivo: Identificar los activos de información institucionales, determinar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información y formular un Plan de Tratamiento que establezca las estrategias y controles a implementar.

6.3.1.1. Flujograma Etapa 1: Formulación del Plan de Tratamiento de Seguridad de la Información año t+1.



6.3.1.2. Matriz Etapa 1: Formulación del Plan de Tratamiento de Seguridad de la Información año t+1.

N°	¿Quién?	¿Qué?	¿Cuándo?	¿Cómo?	Registro
1	Encargado/a de Seguridad de la Información	Realiza levantamiento de activos de información para el año t.	Segundo trimestre del año en curso.	Identifica los activos de información, y establece, para cada uno de ellos, la ubicación, el responsable o dueño, el soporte y la persona autorizada para su manipulación. La información se registra en la “Planilla Inventario de Activos de Información, año t”.	Planilla Inventario de Activos de Información, año t.

				La actividad se realiza siguiendo los lineamientos definidos en la Política de Administración de Activos de Información.	
2	Encargado/a de Seguridad de la Información	Solicita al/la ECS Inventario de Sistemas y Sitios Web[1].	Segundo trimestre del año en curso.	Solicita, mediante correo electrónico dirigido al/la Encargado/a de Ciberseguridad, la elaboración y envío del Inventario de Sistemas y Sitios Web para el año t.	Correo electrónico.
3	Encargado/a de Ciberseguridad	Elabora y envía Inventario de Sistemas y Sitios Web.	Segundo trimestre del año en curso.	Identifica todos los sitios web o sistemas que se encuentran publicados o expuestos a internet que pertenecen y son administrados por el IND. La información se registra en la "Planilla Inventario de Activos de Información, año t" y se envía mediante correo electrónico, al ESI para consolidación.	Correo electrónico.
4	Encargado/a de Seguridad de la Información	Prioriza activos de información año t.	Segundo trimestre del año en curso.	Consolida y revisa la "Planilla Inventario de Activos de Información, año t". Evalúa la criticidad de los activos identificados y selecciona aquellos que serán priorizados para ser gestionados en el año t+1.	Planilla Inventario de Activos de Información, año t.
5	Encargado/a de Seguridad de la Información	Identifica riesgos asociados a los activos priorizados.	Segundo trimestre del año en curso.	Aplica el proceso de evaluación del riesgo de la SI para definir los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información.	Planilla Inventario de Activos de Información, año t
6	Encargado/a de Seguridad de la Información	Evalúa riesgos asociados a los activos priorizados.	Segundo trimestre del año en curso.	Evalúa la probabilidad de ocurrencia y el impacto de que los riesgos identificados se materialicen. Con esta información, determina el	Planilla Inventario de Activos de Información, año t

[1] De acuerdo con la "Política de Administración de Activos de Información Sistema de Seguridad de la Información", se entenderá por sistemas y sitios web: todos aquellos sitios web o sistemas que se encuentren publicados o expuestos a internet, que pertenecen al Instituto Nacional de Deportes (IND) y son administrados por éste.

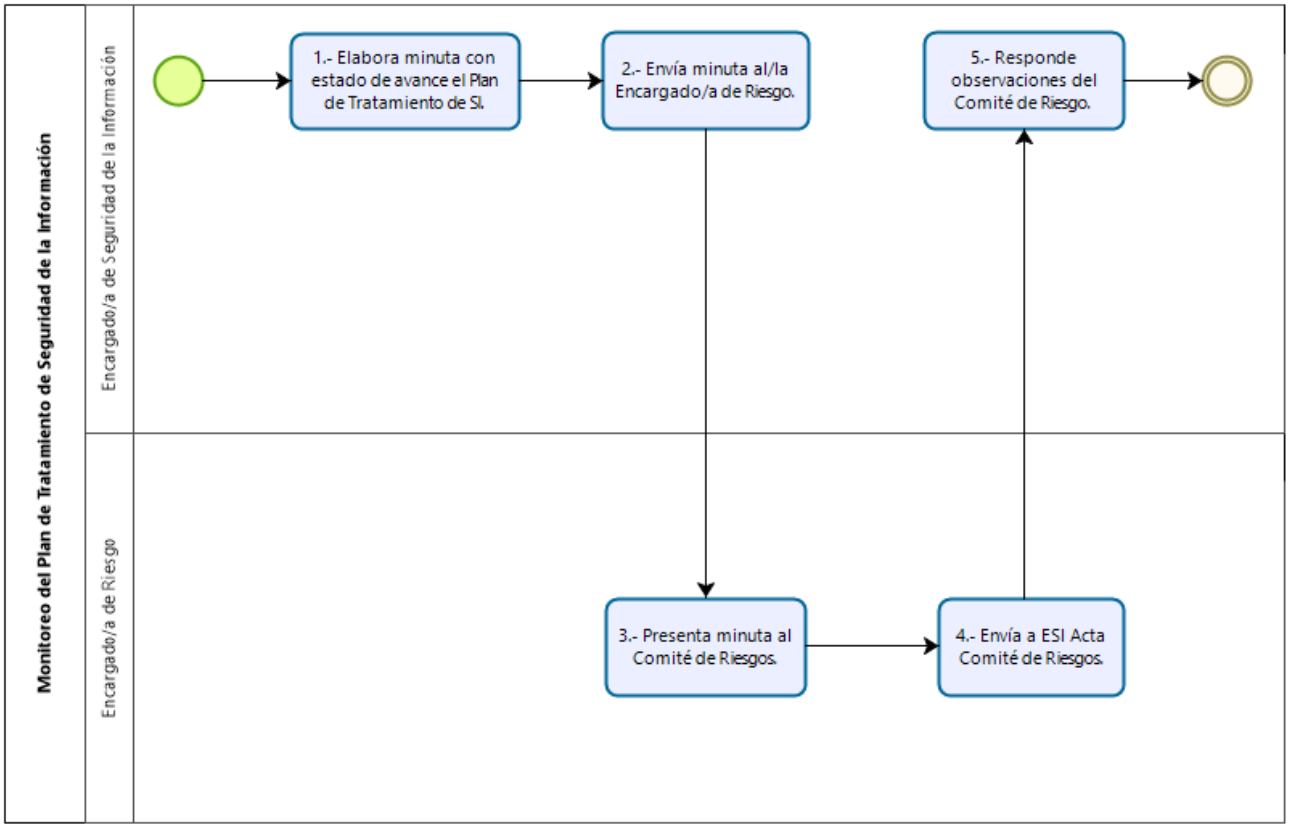
				nivel de riesgo de los activos que fueron priorizados. Adicionalmente, establece los criterios de aceptación del riesgo.	
7	Encargado/a de Seguridad de la Información	Formula Plan de Tratamiento de SI año t+1.	Segundo trimestre del año en curso.	Con apoyo del/la Encargado/a de Ciberseguridad y utilizando como insumo la "Planilla Inventario de activos de Información año t" y la PGSI vigente, se elabora un Plan de Tratamiento para el año t+1. El documento contendrá las estrategias y soluciones específicas para tratar los riesgos, e implementar en los casos que corresponda, los controles que permitirán mitigar los riesgos asociados a los activos de información priorizados el año t.	Plan de Tratamiento de SI año t+1.
8	Encargado/a de Seguridad de la Información	Envía a integrantes del CSI el Plan de Tratamiento de SI año t+1 para revisión.	Segundo trimestre del año en curso.	Envía el Plan de Tratamiento de SI, a través de correo electrónico, a los integrantes del CSI y otorga un plazo aproximado de 1 semana para revisión y ajustes, si corresponde.	Correo electrónico.
9	Comité de Seguridad de la Información	Revisa el Plan de Tratamiento de SI año t+1.	Segundo trimestre del año en curso.	Recibe y revisa el Plan. Si lo estima pertinente, emite observaciones y/o incorpora ajustes. Estas observaciones son enviadas al ESI a través de correo electrónico.	Correo electrónico.
10	Encargado/a de Seguridad de la Información	Recibe observaciones al Plan de Tratamiento de SI año t+1.	Segundo trimestre del año en curso.	Recibe las observaciones y/o comentarios realizados por el CSI y realiza ajustes, si corresponde.	Correo electrónico.

11	Encargado/a de Seguridad de la Información	Cita a sesión al CSI para aprobar Plan de Tratamiento de SI año t+1.	Segundo trimestre del año en curso.	A través de correo electrónico, cita a los miembros del CSI a sesionar para aprobar la versión final del “Plan de Tratamiento de SI año t+1”. Esta sesión puede realizarse de manera online, presencial y/o a través de coordinación mediante correo electrónico, cuando la optimización del tiempo así lo amerite.	Correo electrónico. Acta de sesión CSI.
12	Comité de Seguridad de la Información	Aprueba Plan de Tratamiento de SI año t+1.	Tercer trimestre del año en curso.	En conjunto con el ESI y el ECS revisan la versión final del Plan, lo aprueban y envían al Comité de Riesgo, para su validación.	Correo electrónico.
13	Comité de Seguridad de la Información	Envía Plan de Tratamiento de SI al Comité de Riesgos para validación.	Cuarto trimestre del año en curso.	A través de correo electrónico, envía versión aprobada del Plan de Tratamiento de SI año t+1 a los integrantes del Comité de Riesgos para su validación.	Correo electrónico.
14	Comité de Riesgo	Valida Plan de Tratamiento de SI año t+1.	Cuarto trimestre del año en curso.	Mediante reunión, aprueba el plan de tratamiento de gestión de riesgos y señales de alerta consistente en la implementación de estrategias que permitirán controlar de manera más eficiente la exposición al riesgo de un listado de riesgos y señales de alerta que deben tratarse en el año siguiente, de acuerdo con los lineamientos del CAIGG.	Acta de Reunión
15	Encargado/a de Seguridad de la Información	Respalda documentación validada en carpeta compartida	Cuarto trimestre del año en curso.	Guarda en carpeta compartida de uso institucional, la versión final del Plan de Tratamiento año t+1.	Carpeta compartida.

6.3.2. Etapa 2: Monitoreo del Plan de Tratamiento de Seguridad de la Información año t-1.

Objetivo: Verificar que las estrategias y controles definidos en el Plan de Tratamiento año t-1 se estén implementando de acuerdo al marco regulatorio vigente, e informar periódicamente al Comité de Riesgos respecto al estado de avance del Plan.

6.3.2.1. Flujograma Etapa 2: Monitoreo del Plan de Tratamiento de Seguridad de la Información año t-1.



6.3.2.2. Matriz Etapa 2: Monitoreo del Plan de Tratamiento de Seguridad de la Información.

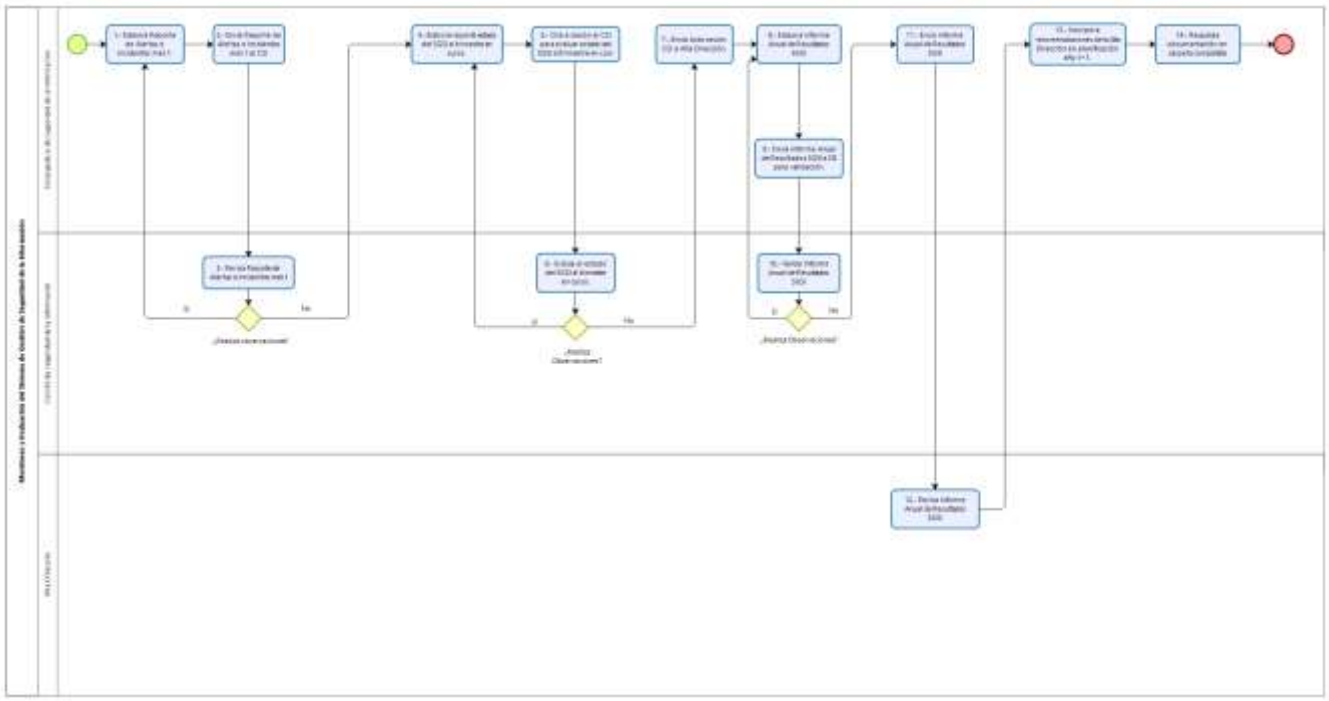
N°	¿Quién?	¿Qué?	¿Cuándo?	¿Cómo?	Registro
1	Encargado/a de Seguridad de la Información	Elabora minuta con estado de avance el Plan de Tratamiento de SI.	Meses de marzo, junio, y septiembre de cada año.	Revisa y evalúa el estado de avance de las estrategias y controles definidos en el Plan de Tratamiento de Seguridad de la Información. Para ello, solicita información a los/las responsables de los activos de información	Correo electrónico. Minuta informativa.

				priorizados y al/la Encargado/a de Ciberseguridad, a través de correo electrónico.	
2	Encargado/a de Seguridad de la Información	Envía minuta al/la Encargado/a de Riesgo.	Meses de marzo, junio, y septiembre de cada año.	Envía, a través de correo electrónico dirigido al/la Encargado/a de Riesgo, la minuta informativa con el estado de avance del Plan de Tratamiento de SI. Este documento, podría incluir información adicional vinculada a la Seguridad de la Información institucional.	Correo electrónico Minuta informativa.
3	Encargado/a de Riesgo	Presenta minuta al Comité de Riesgos.	Meses de abril, agosto y noviembre de cada año.	Durante la sesión, expone los avances informados por el ESI, así como otros temas asociados a la Seguridad de la Información institucional, si corresponde.	Acta Comité de Riesgo.
4	Encargado/a de Riesgo	Envía a ESI Acta Comité de Riesgos.	Meses de abril, agosto y noviembre de cada año.	Envía, a través de correo electrónico dirigido al/la Encargado/a de Seguridad de la Información, el Acta del Comité de Riesgos. En caso de consultas, comentarios, requerimientos de información, etc., éstos son derivados al ESI en el mismo correo.	Correo electrónico.
5	Encargado/a de Seguridad de la Información	Responde observaciones del Comité de Riesgo.	Meses de abril, agosto y noviembre de cada año.	Mediante correo electrónico dirigido al/la Encargado/a de Riesgo, responde a las consultas, comentarios, solicitudes de información, antecedentes u otros, derivados del Comité de Riesgos.	Correo electrónico.

6.4. Subproceso 4: Monitoreo y Evaluación del Sistema de Gestión de Seguridad de la Información institucional.

Objetivo: Revisar el cumplimiento y efectividad del Sistema de Gestión de Seguridad de la Información, a través de la gestión de incidentes y la identificación de oportunidades de mejora; e informar periódicamente a la Alta Dirección respecto a los resultados obtenidos.

6.4.1. Flujograma del Subproceso 4: Monitoreo y Evaluación del Sistema de Gestión de Seguridad de la Información.



6.4.2. Matriz del Subproceso 4: Monitoreo y Evaluación del Sistema de Gestión de Seguridad de la Información.

N°	¿Quién?	¿Qué?	¿Cuándo?	¿Cómo?	Registro
1	Encargado/a de Seguridad de la Información	Elabora Reporte de Alertas e Incidentes mes t.	Mensual	Documenta en forma detallada las alertas y/o incidentes de SI y Ciberseguridad ocurridos en el mes, y evalúa la efectividad de las medidas y controles implementados. Si lo estima pertinente, genera propuestas de mejora.	Reporte/s de Alertas e Incidentes mes t.

2	Encargado/a de Seguridad de la Información	Envía Reporte de Alertas e Incidentes mes t al CSI.	Mensual	Envía el Reporte a través de correo electrónico, a los integrantes del CSI, para su revisión y análisis. Si corresponde, solicita observar las propuestas de mejora levantadas y realizar recomendaciones o proponer ajustes.	Correo electrónico.
3	Comité de Seguridad de la Información.	Revisa Reporte de Alertas e Incidentes mes t.	Mensual	Recibe y revisa el/los Reporte de Alertas e Incidentes. Si corresponde, realiza observaciones, recomendaciones y/o propone ajustes. Estas observaciones son enviadas al ESI a través de correo electrónico.	Correo electrónico.
4	Encargado/a de Seguridad de la Información	Elabora reporte estado del SGSI al trimestre en curso	Meses de marzo, junio y septiembre del año en curso	Documenta en forma detallada las alertas y/o incidentes de SI y Ciberseguridad ocurridos al trimestre vigente, y evalúa la efectividad de las medidas y controles implementados. Si lo estima pertinente, genera propuestas de mejora.	Reporte/s de Alertas e Incidentes al trimestre vigente.
5	Encargado/a de Seguridad de la Información	Cita a sesión al CSI para evaluar estado del SGSI al trimestre en curso.	Meses de marzo, junio y septiembre del año en curso	A través de correo electrónico, cita a los miembros del CSI a sesionar para evaluar el desempeño e implementación del SGSI durante el trimestre. Esta sesión puede realizarse de manera online, presencial, y/o a través de coordinación mediante correo electrónico, cuando la optimización del tiempo así lo amerite.	Correo electrónico.
6	Comité de Seguridad de la Información.	Evalúa el estado del SGSI al trimestre en curso.	Meses de marzo, junio y septiembre del año en curso	En conjunto con el ESI, analiza las principales alertas y/o incidentes ocurridos durante el trimestre y la efectividad de las medidas y controles implementados. Si lo estima pertinente, propone mejoras. Adicionalmente,	Acta de sesión CSI.

				revisa el estado de avance de la planificación interna.	
7	Encargado/a de Seguridad de la Información	Envía Acta sesión CSI a Alta Dirección.	Meses de marzo, junio y septiembre del año en curso	Mediante correo electrónico, envía el Acta de sesión a los integrantes de la Alta Dirección para información y conocimiento. En caso de consultas, comentarios, requerimientos de información, etc., éstos son derivados al ESI, mediante correo electrónico.	Correo electrónico.
8	Encargado/a de Seguridad de la Información	Elabora Informe Anual de Resultados SGSI	Último trimestre del año	Elabora informe con los resultados de la implementación y desempeño del SGSI para el año t. Este documento contendrá, entre otros: - Resumen ejecutivo de las principales alertas y/o incidentes de Seguridad de la Información y Ciberseguridad del año t. - Resultados de la evaluación de riesgo y estado del Plan de tratamiento. - Oportunidades y propuestas de mejora continua.	Informe Anual de Resultados SGSI.
9	Encargado/a de Seguridad de la Información	Envía Informe Anual de Resultados SGSI a CSI para validación.	Último trimestre del año	Envía el Informe a través de correo electrónico a los integrantes del CSI y otorga un plazo aproximado de 1 semana para revisión y ajustes, si corresponde.	Correo electrónico.
10	Comité de Seguridad de la Información	Valida Informe Anual de Resultados SGSI.	Último trimestre del año	Mediante correo electrónico, otorga validación al Informe. En caso de observaciones, envía nuevamente al ESI para ajustes. Una vez incorporados los cambios solicitados, valida el Informe en su versión final.	Correo electrónico.
11	Encargado/a de Seguridad de la Información	Envía Informe Anual de Resultados SGSI.	Último trimestre del año	A través de correo electrónico, envía versión validada del Informe Anual de Resultados SGSI a la Alta Dirección para su	Correo electrónico.

				revisión y evaluación de la conveniencia, suficiencia y efectividad del SGSI en base a los resultados obtenidos.	
12	Alta Dirección	Revisa Informe Anual de Resultados SGSI.	Último trimestre del año	Recibe y revisa el Informe. Si corresponde, entrega lineamientos y/o recomendaciones respecto a las oportunidades de mejora y a cualquier cambio que se requiera implementar. El resultado de la revisión es enviado al CSI y al ESI mediante correo electrónico.	Correo electrónico.
13	Encargado/a de Seguridad de la Información	Incorpora recomendaciones de la Alta Dirección en planificación año t+1.	Último trimestre del año	En conjunto con el CSI, revisa las recomendaciones y lineamientos de la Alta Dirección y los incorpora en la planificación del año t+1.	Planificación año t+1.
14	Encargado/a de Seguridad de la Información	Respalda documentación en carpeta compartida	Último trimestre del año	Guarda en carpeta compartida de uso institucional toda la documentación asociada a la etapa.	Carpeta compartida.

7. Roles y responsabilidades.

Comité de Seguridad de la Información:

- Revisar la Política General de Seguridad de la Información institucional vigente y proponer a la Jefatura Superior del Servicio, si corresponde, su actualización.
- Revisar las Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información institucional y aprobar las versiones vigentes o actualizadas para el año en curso.
- Gestionar los riesgos de Seguridad de la Información de los activos vinculados con los procesos de provisión de productos estratégicos (bienes y servicios).
- Monitorear y evaluar el Sistema de Gestión de Seguridad de la Información institucional e informar periódicamente a la Alta Dirección respecto a los resultados obtenidos.
- Velar por el cumplimiento e implementación de este Procedimiento.

Encargado de Seguridad de la Información:

- Coordinar y apoyar al Comité de Seguridad de la Información en la revisión y propuesta de actualización, de la Política General de Seguridad de la Información institucional.
- Coordinar y apoyar al Comité de Seguridad de la Información en la revisión de las Políticas, Planes y Procedimientos asociados a la Política General de Seguridad de la Información institucional.

- Coordinar y apoyar al Comité de Seguridad de la Información en la gestión de riesgos de Seguridad de la Información, asociados a activos de información institucionales.
- Coordinar y apoyar al Comité de Seguridad de la Información en el monitoreo y evaluación del Sistema de Gestión de Seguridad de la Información institucional, a través de la gestión de incidentes y la identificación y propuesta de oportunidades de mejora.
- Velar por el cumplimiento e implementación de este Procedimiento.

Encargado de Ciberseguridad (ECS):

- Apoyar al Comité de Seguridad de la Información y al Encargado de Seguridad de la Información, en la gestión de riesgos de Seguridad de la Información, asociados a los activos de información institucionales.
- Apoyar al Comité de Seguridad de la Información en el monitoreo y evaluación del Sistema de Gestión de Seguridad de la Información institucional, a través de la gestión de incidentes y la identificación y propuesta de oportunidades de mejora.

Alta Dirección:

- Desplegar los medios técnicos, financieros y humanos para garantizar la correcta implementación del SGSI.
- Apoyar las operaciones y medidas que se tomen ante cualquier evidencia de incumplimiento, ineficiencia e ineficacia.

8. Identificación de riesgos.

Nro.	Riesgo asociado
1	Incumplimiento de los plazos establecidos en el Plan de Trabajo.
2	Rotación en los Integrantes del Comité de Seguridad de la Información.
3	Cambio en la legislación vigente en materias de Seguridad de la Información.
4	No contar con un equipo de respuestas ante incidentes de Seguridad de la Información.
5	Cambio en los objetivos y de las prioridades institucionales.
6	Concentrar la distribución de actividades y responsabilidades en una cantidad reducida de personal, generando sobrecarga laboral.

9. Recursos.

- Recurso humano capacitado en materias de Seguridad de la Información y Ciberseguridad.
- Equipamiento de software y hardware para la Gestión de Incidentes de Seguridad.
- Políticas y procedimientos en materias de Seguridad de la Información.

10. Registros.

- Actas de sesión del Comité de Seguridad de la Información.
- Reporte de Alertas e Incidentes.

- Informe Anual de Resultados SGSI.
- Correo electrónico.
- Carpeta compartida de uso institucional.
- Plataforma
- Plan de Revisión año t.

11. Indicadores de procesos.

Nº	INDICADOR	FORMULA DE CALCULO	MEDIO DE VERIFICACIÓN	FRECUENCIA DE MEDICION	RANGO DE DESEMPEÑO		
					OPTIMO	NORMAL	DEFICIENTE
1	Porcentaje de reuniones del Comité de Seguridad de la Información.	(N° de reuniones del Comité de Seguridad realizadas / N° de reuniones del Comité de Seguridad planificadas) *100	Acta de Reunión	Trimestral	100%	>=90 %	<90 %
2	Porcentaje de Incidentes de seguridad resueltos	(N° de incidentes de seguridad resueltos / N° de incidentes de seguridad registrados) *100	Formulario de Registro de Incidentes	Mensual	100 %	>=90 %	<90 %
3	Porcentaje de difusiones de seguridad de la información realizadas	N° de difusiones de seguridad de la información realizadas / N° de difusiones de seguridad de la información planificadas) *100	Boletín de Comunicaciones	Mensual	100 %	>=90 %	<90 %

12. Anexos.

- Formulario de Registro de incidente de Seguridad de la Información.
- Informe Anual del Sistema de Gestión de Seguridad de la Información

CUMPLIMIENTO INSTRUCTIVO PRESIDENCIAL Nº 8

INFORME DE INCIDENTES DE SEGURIDAD REGISTRADOS DURANTE EL MES DE _____ AÑO_____.

Instituto Nacional de Deportes
Ministerio del Deporte
Gobierno de Chile

Respuesta ante Incidentes Informáticos

A continuación, se detallan los incidentes reportados por el CSIRT de Gobierno y respondidos conforme a lo establecido en el IP N°8.

Cantidad de Incidentes reportados: **0**
Cantidad de incidentes registrados: **0**
Cantidad de incidentes solucionados: **0**

No se registran incidentes durante el mes _____ año _____ .

Aprobaciones

Función	Nombre	Cargo	Firma
Responsable de Elaboración		Encargado de Seguridad de la Información – IND	

INFORME ANUAL DE GESTIÓN DE INCIDENTES
Sistema de Gestión de Seguridad de la Información y Ciberseguridad

1. OBJETIVO

Entregar información consolidada de los incidentes y/o debilidades en materias de seguridad de la información y/o Ciberseguridad, ocurridos en el IND en el año en curso, realizando el análisis y las recomendaciones de mejora correspondientes

2. ALCANCE

Incidentes y debilidades ocurridas durante el período de tiempo comprendido entre el XX/XX/XXXX y el XX/XX/XX. Los últimos 15 días del mes de diciembre serán incluídos en el informe correspondiente al año XXXX.

3. RESUMEN

Período:	XX/XX/XXXX al XX/XX/XXXX
Cantidad de incidentes:	X
Cantidad de debilidades:	X
Tipos de activos afectados:	Equipamiento
	Sistema
	Información

4. DETALLE DE LOS INCIDENTES

Número	1
Descripción del incidente	
Fecha del incidente	
Tipo de incidente	
Alcance - Sistemas afectados	
Impacto	
Prioridad	
Amenaza	
Activo afectado	
Como se detecto el incidente	
Respuesta o escalamiento del incidente	
Causa del incidente	
Accion correctiva	
Descripción de evidencia	

Número	2
Descripción del incidente	
Fecha del incidente	
Tipo de incidente	
Alcance – Sistemas afectados	
Impacto	
Prioridad	
Amenaza	
Activo afectado	
Como se detecto el incidente	
Respuesta o escalamiento del incidente	
Causa del incidente	
Accion correctiva	
Descripción de evidencia	

Número	3
Descripción del incidente	
Fecha del incidente	
Tipo de incidente	
Alcance – Sistemas afectados	
Impacto	
Prioridad	
Amenaza	
Activo afectado	
Como se detecto el incidente	
Respuesta o escalamiento del incidente	
Causa del incidente	
Accion correctiva	
Descripción de evidencia	

Número	4
Descripción del incidente	
Fecha del incidente	
Tipo de incidente	
Alcance – Sistemas afectados	
Impacto	
Prioridad	
Amenaza	

Activo afectado	
Como se detecto el incidente	
Respuesta o escalamiento del incidente	
Causa del incidente	
Accion correctiva	
Descripción de evidencia	

5. CONCLUSIONES:

Indicador:

$$\%\ de\ incidentes\ resueltos = \frac{nº\ de\ incidentes\ resueltos}{nº\ incidentes\ informados} = \frac{4}{4} = 100\%$$

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración			
Responsable de Revisión y Aprobación			
Responsable de Revisión y Aprobación			
Responsable de Revisión y Aprobación			
Responsable de Revisión y Aprobación			

Control de Cambios

Versión	Fecha	Responsable	Descripción
1			