1. OBJETIVO

Identificar los activos de información institucionales y definir las responsabilidades y nivel de protección adecuada de acuerdo a su criticidad dentro de los procesos, de acuerdo a la norma NCh-ISO 27001:2013, de manera de resguardar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

La presente política define la administración de los activos de información críticos vinculados a cada una de las etapas de los procesos de provisión vigentes en el IND, que dan soporte a los productos estrátegicos institucionales, de acuerdo a lo establecido en la Ficha de Definiciones estratégicas (A1).

3. MATERIAS ESPECÍFICAS QUE ABORDA

- A.08.01.01 Inventario de activos
- A.08.01.02 Propiedad de los activos
- A.08.01.04 Devolución de activos
- A.08.02.01 Clasificación de información

4. ROLES Y RESPONSABILIDADES

- Comité de Seguridad de la Información
  - Velar por el cumplimiento y actualización de la presente Política de Administración de Activos de Información.
- Encargado/a de Seguridad de la Información
  - Mantener, actualizar y custodiar el Inventario de Activos de Información.
- Encargado/a de Ciberseguridad
  - Mantener, actualizar y custodiar el Inventario de Sistemas y Sitios Web
- Jefaturas de área
  - Determinar y clasificar los activos de información críticos o relevantes de su área, de acuerdo a los declarados en el alcance de esta política.
- Funcionarios:
  - Velar por mantener la integridad, confidencialidad y disponibilidad de los activos de información que están a su cargo, cuidando de su buen uso y realizando su correcta devolución una vez terminada la relación laboral con la institución.

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 esta Política. En ambos casos, estas revisiones y evaluaciones serán en la sesiones del Comité de Seguridad de la información.

6. DIFUSIÓN

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

7. DEFINICIONES

- 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.
- Integridad de la Información: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- Confidencialidad de la Información: Es la propiedad que impide la divulgación de información a personas, entidades o procesos no autorizados.
- Disponibilidad de la Información: es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

8. POLITICA

8.1 Inventario de activos de información

8.1.1 Inventario de activos de información

El Instituto Nacional de Deportes (IND) proporciona a los funcionarios y terceros autorizados activos de información institucionales para cumplir con sus objetivos.

Todos los activos de información considerados en el alcance deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requisitos y los criterios que dicte la presente política.

El levantamiento de activos de información debe consolidarse en un inventario, el cual debe incluir la siguiente información referente a cada uno de los activos de información identificados:

- Proceso: corresponde al nombre del proceso de negocio (de provisión de productos/servicios estratégicos) al cual pertenecen los activos de información a incluir en el inventario.
- Subproceso: son aquellos subprocesos en los que puede estar dividido el Proceso, dependiendo de la complejidad del mismo.

- Etapa relevante: detalle de las fases más importantes que se deben desarrollar en cada subproceso para dar origen a los productos.
- Nombre del activo de información: en este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características.
- Tipo de activo (estos pueden ser):
    - Documento: corresponde a un escrito que refleja el resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella. Este puede ser físico o electrónico.
    - Base de Datos: es la información sistematizada y organizada.
    - Formulario: corresponde a documentos utilizados para recoger información.
    - Software: programa computacional empaquetado producido por una empresa que lo comercializa.
    - Sistema: programa computacional a medida, desarrollado por la institución o por un externo, cuyo objetivo es apoyar un proceso de negocio.
    - Equipos: objetos o dispositivos que realizan o apoyan la realización de una función.
    - Infraestructura Física: estructura que permite almacenar y/o custodiar activos de información del proceso, tales como: datacenter, oficina de partes, bodegas, caja fuerte, etc.
    - Expediente: conjunto de documentos y formularios dispuestos en estricto orden de ocurrencia, de ingreso o egreso. Este puede ser físico o electrónico.
- Ubicación: corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.
- Responsable/Dueño: corresponde al rol a cargo de la persona autorizada para tomar decisiones respecto del activo. Esto implica necesariamente derecho de propiedad sobre el activo.
- Soporte: corresponde al medio en el cual se encuentra registrado el activo, este puede ser en papel o digital.
- Persona autorizada para manipular: corresponde al rol a cargo de la(s) persona(s) autorizada(s) para usar el activo de información, ya sea modificándolo, actualizándolo o trasladándolo.

8.1.2 Inventario de Sistemas y Sitios Web - Ciberseguridad

Se debe realizar un levantamiento de todos aquellos sitios web o sistemas que se encuentran publicados o expuestos a internet que pertenecen y son administrados por el IND, por ejemplo:

- Sitio web institucional e informativos expuestos a intenet (por ejemplo: sitios de consulta ciudadana, portales de postulación, entre otros).
- Servicios Cloud que incluyan sistemas, servicios web, mail institucional (por ejemplo: Office 365, Amazon, Gmail Empresa, etc.)
- Portales VPN, webmail institucional, sitios FTP.
- Sistemas propios de la gestión institucional, publicados a Internet (por ejemplo: servicios de mensajería, repositorios de documentos, repositorios de firmas, portales de RRHH, plataformas de uso de fiscalizadores, entre otros.)

Para cada sistema o sitio web se debe identificar la siguiente información:

- Si cuenta o no con una solución de alta disponibilidad (servidores o sistemas replicados en una ubicación distinta, en modalidad activo-activo o activo-pasivo). Incluye ubicación física para los sistemas de alta disponibilidad (por ejemplo: ubicación datacenter primario y secundario)
- Sistema operativo instalado en los servidores de ambas capas, incluyendo versión y si existe contrato vigente con proveedor o marca.
- Motor de bases de datos, incluyendo versión y si existe contrato vigente con proveedor o marca.
- Almacenamiento de datos personales, ya sean de sus funcionarios o usuarios externos.
- Existencia de servicios cloud (para sitio web, correo, plataformas especificas, etc.)
- Si los sistemas o sitios web fueron desarrollados dentro de la institución o por un proveedor externo.
- Lenguaje utilizado en el sistema o sitio web (por ejemplo: PHP, JavaScript, entre otros).
- Si se aplica metodologías de desarrollo seguro (por ejemplo: OWASP).
- Si utiliza webservices para la comunicación con otros sistemas.
- Vigencia de soporte.
- Evaluación de componentes de Software a través de Herramientas (por ejemplo: Nessus, Accunetix, entre otros).
- Evaluaciones de configuraciones y reglas de negocio a través de Ethical Hacking.

8.2 Propiedad de los activos de información

Los activos mantenidos en el inventario deben tener asignado un responsable o dueño, quien es responsable de la administración correcta de un activo durante todo su ciclo de vida.

Entre las funciones y responsabilidades de los propietarios de los activos de información se encuentran las siguientes:

- Garantizar que se realice un inventario de todos los activos que tiene a su cargo.
- Clasificar los activos de información según su grado de confidencialidad, integridad y disponibilidad.
- Definir y revisar periódicamente las restricciones de acceso y clasificaciones para los activos críticos, considerando las políticas control de acceso pertinente.
- Asegurarse de un manejo adecuado cuando se elimine o destruya un activo.

Se puede delegar las tareas rutinarias a un custodio que resguarde los activos diariamente, pero la responsabilidad sigue siendo del propietario.

En sistemas de información complejos, se puede asignar grupos de activos que actúen en conjunto para brindar un servicio en particular. En este caso el propietario de este servicio es responsable de la entrega del servicio, incluida la operación de sus activos.

8.3 Devolución de activos de información

Todos los funcionarios y usuarios externos deben devolver todos los activos de información previamente entregados y que están en su poder al finalizar su empleo, contrato o acuerdo. Esta devolución debe ser formalizada al momento de la desvinculación o egreso.

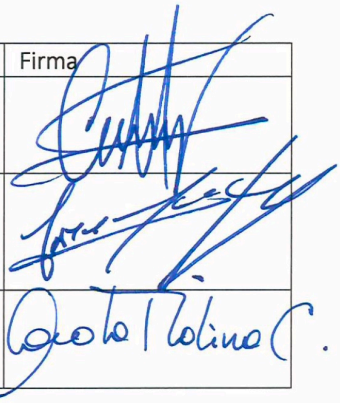
En los casos donde el funcionario o el mismo externo cuenta con conocimiento importante para las operaciones continuas, dicha información se debe documentar y transferir a la institución, a través de las jefaturas correspondientes.
Durante el período de aviso de desvinculación, término de contrato o de egreso según sea el caso, se deben controlar las copias no autorizadas de la información pertinente (es decir, propiedad intelectual) de los funcionarios y usuarios externos desvinculados o en egreso.

8.4 Clasificación de información

Los propietarios de los activos de información son los responsables de clasificar sus activos, de acuerdo a las condiciones de confidencialidad, integridad y disponibilidad que ellos presentan. Los activos de clasificarán según las siguientes categorías:

- Confidencialidad:
  - Pública: activo no tiene restricciones de acceso.
  - Reservada: activo de información cuyo acceso no autorizado tiene un alto impacto para la institución o terceros.
- Integridad
  - Baja: activo de información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
  - Media: activo de información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
  - Alta: activo de información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros.
- Disponibilidad
  - Baja: activo de información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.
  - Media: activo de información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.
  - Alta: activo de información cuya inaccesibilidad, tiene impacto grave para la institución o terceros.

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración	Cristian Villalobos Zamora	Encargado PMG Seguridad de la Información	
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 0.1	18-07-2017	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento para dar cumplimento al PMG-SSI 2017 y abordar requerimientos internos del IND.
Versión 1.0	02-07-2018	Cristian Villalobos Z.	Se modifica la difusión de la política y se ajustan las responsabilidades.
Versión 2.0	16-05-2019	Cristian Villalobos Z.	Se incluye el inventario de sistemas y sitios web, alineado con el IP nº8 de Ciberseguridad.