1. OBJETIVO

El objetivo de la Presente Política es establecer los lineamientos para una administración eficiente y segura de las operaciones en la infraestructura tecnológica del Instituto Nacional de Deportes (IND), teniendo como base los objetivos de control de la Norma NCh-ISO 27001:2013.

2. ALCANCE

La presente política aplica a la plataforma tecnológica que soporta todos los procesos de provisión vigentes en el Instituto Nacional de Deportes (IND), de acuerdo a lo establecido en la Ficha de Definiciones Estratégicas (A1).

3. DOCUMENTOS RELACIONADOS

- Norma NCh-ISO 27001:2013
- Política General de Seguridad de la Información

4. MATERIAS ESPECIFICAS QUE ABORDA

La presente Política está asociada a los siguientes controles de la norma NCh-ISO 27001:2013

- A.12.01.01: Procedimientos operativos documentados.
- A.12.01.04: Separación de entornos de desarrollo, pruebas y operacionales.
- A.12.02.01: Controles contra el malware.
- A.12.03.01: Respaldo de Información.
- A.12.04.01: Registros de eventos.
- A.12.04.02: Protección de registro de información.
- A.12.04.03: Registros del administrador y del operador.
- A.12.04.04: Sincronización con relojes.
- A.12.05.01: Instalación de software en sistemas operacionales.
- A.12.06.02: Restricciones en la instalación de software.
- A.12.07.01: Controles de auditoría de los sistemas de información.

5. ROLES Y RESPONSABILIDADES

- Encargado/a de Seguridad de la Información:
  - Asesorar al Jefe de Servicio en materias de Seguridad de la Información.
  - Monitorear el avance general de la implementación de las estrategias de control y tratamiento de los riesgos asociados a la Seguridad de la Información.
  - Es responsable del cumplimiento, ciclo de vida y actualización de la presente Política.

- Comité de Seguridad de la Información:
  - Velar por la correcta implementación de los controles de seguridad mencionados en la presente Política.

- Departamento de Informática:
  - Administrar la plataforma tecnológica del IND cumpliendo las clausulas establecidas en la presente política.
  - Aplicar la normativa de seguridad a la plataforma tecnológica del IND.

6. REVISIÓN Y EVALUACIÓN

La presente Política debe ser objeto de revisión y de evaluación en relación con su correcta aplicación cuando se cumpla un año 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 realizadas en las sesiones del Comité de Seguridad de la Información.

7. DEFUSIÓN

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

8. DEFINICIONES

- Norma NCh-ISO 27001:2003: define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de una organización.
- Control A.12.01.01: los procedimientos operativos se deberían documentar y dejar a disposición de todos los usuarios que los necesiten.
- Control A.12.01.04: los entornos de desarrollo, pruebas y operacionales se deberían separar para reducir los riesgos de acceso o cambios no autorizados al entorno operacional.
- Control A.12.02.01: se deberían implementar controles para la detección, prevención y recuperación para resguardarse contra el malware.
- Control A.12.03.01: se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada.

- Control A.12.04.01: se deberían producir, mantener y revisar de manera periódica los registros de eventos del usuario, las excepciones, las fallas y los eventos de seguridad de la información.
- Control A.12.04.02: las instalaciones de registros y la información de registro deberían estar protegidas contra la adulteración y el acceso no autorizado.
- Control A.12.04.03: las actividades del administrador y del operador del sistema se deberían registrar y los registros se deberían proteger y revisar de manera regular.
- Control A.12.04.04: se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad con una fuente de tiempo de referencia única.
- Control A.12.05.01: se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.
- Control A.12.06.02: se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
- Control A.12.07.01: se deberían planificar y acordad los requisitos y las actividades de auditoria que involucran la verificación de los sistemas operacionales para minimizar las interrupciones a los proceso comerciales.

9. POLÍTICA

9.1 Documentación de Procedimientos de operación

Se deben documentar y mantener actualizados los procedimientos operativos identificados en la presente Política y sus cambios será aprobado por el Comité de Seguridad de la Información. Los procedimientos especificaran instrucciones para la ejecución detallada en las siguientes áreas de aplicación:

- Procesamiento y manejo de información.
- Respaldo de información.
- Monitoreo de los sistemas.
- Los requisitos de programación, incluidas las interdependencias con otros sistemas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de las tareas.
- Restricciones en el uso de aplicaciones utilitarias del sistema.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Reinicio del sistema y procedimiento de recuperación en caso de producirse fallas en el sistema.

9.2 Separación de entornos de desarrollo, prueba y producción

Los ambientes de desarrollo, prueba y producción, siempre que sea posible, estarán separados de forma física y/o lógica, y se definirán y documentaran las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo. Se deben considerar los siguientes requisitos.

- Se debe evitar realizar pruebas en los sistemas del ambiente de producción.
- No se deberían copiar datos sensibles en el entorno del sistema de pruebas a menos que se entreguen controles de acceso equivalentes al sistema de producción.

9.3 Controles contra virus y código malicioso

Se debe implementar controles para la detección, prevención y recuperación antes los ataques de virus y código malicioso, en combinación con la concientización adecuada para los usuarios. Se establecen como requerimientos de seguridad en este ámbito los siguientes puntos:

- La plataforma de red de datos del IND debe contar con un software de detección de virus y código malicioso, que brinde reparación y análisis de computadores y medios como control de precaución para taques de esa naturaleza.
- Implementar controles que eviten o detecten el uso de sitios web desconocidos o que se sospecha que son maliciosos.
- Se debe analizar datos adjuntos de correos electrónicos en busca de código malicioso antes de su uso; este análisis se debería realizar en diferentes lugares, es decir, en servidores de correo electrónico, computadores de escritorio y al ingresar a la red datos del IND.
- Se deben crear políticas que restrinjan las instalaciones de software no autorizado por parte de los usuarios.

9.4 Respaldo de información

El Instituto Nacional de Deportes (IND), debe contar con un sistema de respaldo de información que permita la recuperación ante un desastre:

- Se definirá y documentará los controles para la ejecución de tareas programadas para la generación de respaldos de información, la cual debe ser administrada y revisada constantemente.
- El Área de Operaciones del IND, dispondrá y controlará la realización de dichas copias o respaldos.

- Se debe contar con instalaciones de resguardo que garanticen la disponibilidad de la información y del software crítico del IND.
- El software de respaldo deberá probarse periódicamente, asegurándose que cumplen con los requisitos de continuidad operacional de la institución.

9.5 Registro y Gestión de eventos

- Debe monitorearse el uso de las instalaciones de procesamiento de información, debiendo generar, mantener y revisar los registros de las actividades de los usuarios; excepciones, fallas y eventos de seguridad de la información.
- Tanto los sistemas de monitoreo, como la información registrada durante las actividades de monitoreo deben ser protegidos contra la alteración indebida y el acceso no autorizado.
- Se deben realizar revisiones regulares y detalladas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Se debe llevar a cabo actividades para el registro de actividades, incluyendo según corresponda:
    - Elaboración del registro de fallas reportadas por usuarios, programas y sistemas, con el objetivo de prevenir su repetición o facilitar su resolución en caso de reincidencia.
    - Registro y revisión de las medidas correctivas tomadas.
    - Revisión de registro de fallas para asegurar que los problemas han sido satisfactoriamente resueltos.
    - Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
    - Ejecución de operaciones críticas.
    - Cambios a información crítica.
- Se deben registrar, respaldar, proteger y revisar regularmente, las actividades del administrador y operadores de las distintas plataformas tecnológicas. El log de actividades debe incluir al menos:
    - Identificación del equipo.
    - horario de arranque y finalización de los procesos del sistema.
    - Errores del sistema y acciones críticas realizadas por la cuenta del operador que realizó la actividad, sistemas y procesos involucrados.

9.6 Sincronización de relojes

Los relojes de todos los elementos relevantes de redes y sistemas de procesamiento de información, deben estar configurados apropiadamente y sincronizados respecto de una fuente de tiempo precisa.

El Área de Operaciones, debe definir el procedimiento para la configuración y sincronización de los relojes de los equipos de red y sistemas de información del IND.

9.7 Control sobre la instalación de software en sistemas de producción

Con el fin minimizar los riesgos de alteración, se debe controlar la instalación de software en los sistemas operacionales. Los requerimientos de seguridad para la instalación de software en los sistemas de producción se describen a continuación:

- Los sistemas operativos y el software de aplicación solamente deben ser implementados en producción después de superar pruebas relativas a la utilización, seguridad, efectos sobre otros sistemas y usabilidad, ejecutadas en sistemas separadas. Adicionalmente, se debe asegurar que todas las correspondientes librerías fuente de los programas hayan sido actualizadas.
- Debe implementarse un sistema de control de configuración para mantener el control del software implementado y la documentación de los sistemas de información del IND.
- Debe existir una estrategia de reversión antes de iniciar la implementación de cambios.
- Debe mantenerse un registro de auditoria de las actualizaciones realizadas sobre las librerías de programas operativos.
- Las versiones previas del software aplicativo deben ser retenidas como medida de contingencia.
- Las versiones antiguas de software debe ser archivadas juntamente con toda la información requerida, parámetros, procedimientos, detalles de configuración y software de soporte durante el mismo periodo que se requiera retener los datos.
- El software utilizado en ambientes de producción provistos por terceros debe ser mantenido en un nivel de versión soportado técnicamente por el proveedor.
- Toda decisión de actualización debe tomar en cuenta las necesidades operativas para instrumentar el cambio, la estabilidad y la seguridad de la actualización, es decir, analizar los beneficios de la introducción de nuevas funcionalidades de seguridad y el número y la severidad de los problemas de seguridad que afectan a la versión.
- Los parches de software deben ser aplicados a los ambientes de producción cuando ayuden a eliminar o reducir las debilidades de seguridad y hayan sido previamente testeados en un ambiente de pruebas.

- El acceso físico y lógico solamente debe ser otorgado a los proveedores con propósitos de soporte cuando sea necesario, con aprobación expresa, y sus actividades deber ser monitoreadas.
- Coordinar la implementación de modificaciones o nuevos programas en el ambiente de producción.

9.8 Instalación de software en estaciones de trabajo

La instalación de software en estaciones de trabajo, es solo labor y responsabilidad del Área de Operaciones, aplicando para los usuarios el principio de menor privilegio y privilegio de restringido.

- Los funcionarios no están facultados para realizar la instalación y utilización de software no autorizado en sus estaciones de trabajo y en las plataformas tecnológicas que soportan los sistemas de información del IND.
- La instalación no controlada de software en la plataforma de computadores del IND, será considerada como una amenaza que puede traer consigo riesgos de seguridad generados por la aparición de vulnerabilidades, fuga de información, incidentes de integridad y transgresión a derechos de propiedad intelectual.

9.9 Controles de auditoría de los sistemas de información

- Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar detalladamente para minimizar el riesgo de interrupciones de los procesos de negocio.
- Se protegerá el acceso a los elementos utilizados en las auditorias de sistemas, es decir, archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y desarrollo, y se les otorgará el nivel de protección requerido.

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	06-10-2016	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento su aplicación y cumplimiento al PMG-2017 y abordar requerimientos internos del IND-
Versión 2	02-07-2018	Cristian Villalobos Z.	Se modifica el formato, la difusión de la política y las responsabilidades.
Versión 3	16-05-2019	Cristian Villalobos Z.	Se reemplaza en nombre Unidad de Coordinación Informática por Departamento de Informática.