1. OBJETIVO

Esta Política tiene como propósito establecer los lineamientos de seguridad para la gestión del desarrollo, mantención y adquisición de sistemas de información en el Instituto Nacional del Deporte (IND).

2. ALCANCE

Esta política se aplica a los sistemas de información desarrollados en la institución y por terceros, que soportan la operación de los procesos de provisión de bienes y servicios de la institución, 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.14.01.01 Análisis y especificación de los requisitos de seguridad de la información.
- A.14.01.02 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- A.14.02.01 Política de desarrollo seguro.
- A.14.02.06 Seguridad en entornos de desarrollo.
- A.14.02.08 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- A.14.02.09 Pruebas de aceptación

5. ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información:

- Ser responsable del ciclo de vida de la presente Política.
- Velar por el cumplimiento y actualización del presente Política.

Encargado de Seguridad de la Información:

- Definir los requerimientos de seguridad para sistemas nuevos, antes de la etapa de desarrollo.
- Validar el cumplimiento de esta política y de los requisitos de seguridad en los sistemas.
- Velar por el seguimiento de las vulnerabilidades técnicas.
- Presentar al Comité de Seguridad de la Información las vulnerabilidades técnicas asociadas a presupuesto para su solución.

Área de Desarrollo:

- Ceñirse a las indicaciones que la presente normativa con relación al desarrollo seguro y cumplimiento en relación con la detección de vulnerabilidades técnicas.
- Incorporar a las pruebas funcionales de los sistemas, las pruebas de seguridad.
- Gestionar revisiones de vulnerabilidades técnicas a los sistemas de IND antes de salir a producción.
- Responsable del seguimiento y reparación de las vulnerabilidades técnicas detectadas.
- Velar por las capacidades de los desarrolladores de evitar, encontrar y solucionar vulnerabilidades técnicas.

Proveedores IND

- Ceñirse a las indicaciones que la presente normativa exige en relación con el desarrollo seguro y cumplimiento para la correcta detección y mitigación de vulnerabilidades técnicas.
- Asegurar el adecuado cumplimiento de las competencias técnicas en desarrollo seguro de sistemas de todo el equipo asignado.

6. 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 realizadas en las sesiones del Comité de Seguridad de la Información.

7. DIFUSIÓN

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

8. POLITICA

8.1 ESPECIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD

- Para la construcción de nuevos sistemas de información o mejoras a los existentes, se debe especificar los controles de seguridad desde la etapa de levantamiento de requerimientos, tales como perfiles de acceso, autenticación, encriptación de claves, auditoria de trazabilidad; entre otros.

- En la identificación de controles de seguridad deben participar las áreas de negocio que serán usuarios del sistema de información en construcción o proceso de mantención.

- El diseño e implementación de controles de seguridad deben ser preferentemente de tipo automático, evitando procesos o intervención manuales. Las excepciones deben ser aprobadas por el Encargado de Seguridad de la Información.

- En la etapa de diseño, debe considerarse los procedimientos necesarios para realizar revisiones periódicas de contenidos de campos, registros, tablas (de datos), o archivos considerados sensibles, frecuencia de los respaldos y tiempos de retención de estos, y procesos de depuración (limpieza de datos, indexaciones, u otros procesos relacionados con optimización y rendimiento).

- Se puede emplear datos de prueba extraídos desde las bases de datos de los sistemas en producción, pero sólo deben ser empleadas dentro de las instalaciones de IND. Excepciones a esta política, deben ser autorizadas por el dueño de la información, o en su defecto por el Encargado de Seguridad de la Información y se deberá elaborar y formalizar un Acuerdo de Confidencialidad por parte de terceros.

- El acceso a las bases de datos de construcción prueba y producción, deben contar con controles de acceso (autenticación y autorización). Debe definirse quiénes (roles) tienen acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación). Jamás en la etapa de construcción y/o prueba se debe dar acceso a los datos de producción.

8.2 ENTORNO DE DESARROLLO SEGURO

- IND debe establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo de sistemas. Esto implica un control de acceso restringido al entorno de desarrollo y al código fuente.

- Un entorno de desarrollo seguro incluye a las personas, procesos y tecnologías asociadas con el desarrollo e integración de sistemas.

- El Área de Desarrollo en conjunto con el Encargado de Seguridad de la Información deberán evaluar los riesgos asociados con las labores de desarrollo de sistemas individuales y establecer entornos de desarrollo seguro, para ello se debe considerar los siguientes elementos:

    - La sensibilidad de los datos que el sistema procesará almacenará y transmitirá.
    - Los requisitos externos e internos correspondientes, es decir, de las normativas o políticas.
    - Controles de seguridad que ya ha implementado la organización y que soportan el desarrollo del sistema.
    - Confiabilidad del personal que trabaja en el entorno.
    - El grado de externalización asociado al desarrollo del sistema
    - La necesidad de contar con segregación entre distintos entornos de desarrollo
    - Control del acceso al entorno de desarrollo
    - Monitoreo del cambio al entorno y al código que ahí se almacena
    - Que los respaldos se almacenen en ubicaciones fuera del sitio
    - Control sobre el movimiento de datos desde y hacia el entorno.
    - La documentación requerida en las diferentes etapas de ciclo de vida de los sistemas.

8.2 REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON REDES PÚBLICAS

Las transacciones de servicios deberán ser protegidas para evitar la transmisión incompleta de información, el enrutamiento incorrecto, la alteración, divulgación y duplicación no autorizada de mensajes.

Los servicios de aplicación que pasan a través de redes públicas deben ser adecuadamente protegidos de actividades fraudulentas, protegiendo la confidencialidad, integridad y disponibilidad de la información que se transfiere a través de los mismos.

Para cumplir estos requerimientos se definen dos responsabilidades:

- El Departamento de Informática es el responsable de definir los controles de seguridad relacionados con la información en los servicios de aplicaciones que se transmiten sobre redes públicas:
    - La descripción de los sistemas de autenticación que se usarán.
    - La descripción de cómo se garantizarán la confidencialidad e integridad de la información.
    - La descripción de cómo se garantizarán las acciones de inviolabilidad.

- Cuando la institución requiera la implementación de servicios de transacción en línea, la Unidad de Coordinación Informática será la responsable de la definición de controles, los cuales deben incluir los siguientes:
    - Cómo se evitará el direccionamiento erróneo.
    - Cómo se evitará la transmisión de datos incompletos.
    - Cómo se evitará la modificación no autorizada de mensajes.
    - Cómo se evitará la duplicación no autorizada de mensajes.
    - Cómo se evitará la divulgación no autorizada de datos.

8.3 PRINCIPIOS DE INGENIERIA SEGURA EN SISTEMAS

- Se deberán establecer, documentar y aplicar los procedimientos de desarrollo de sistemas de información seguro en base a los principios de ingeniería de seguridad en las actividades de ingeniería del sistema de información interno. La seguridad se debería diseñar en todos los niveles de la arquitectura (negocios, datos, aplicaciones y tecnología) equilibrando la necesidad de la seguridad de la información con la necesidad de accesibilidad.

- Se debe analizar la tecnología nueva para conocer sus riesgos de seguridad y el diseño se deber revisar contra los patrones de ataque conocidos.

- Estos principios y los procedimientos de ingeniería establecidos se deben revisar de manera regular para asegurarse de que contribuyen de manera eficaz a las normas de seguridad mejoradas dentro del proceso de ingeniería.

8.4 PRUEBAS DE SEGURIDAD

- Los sistemas nuevos y actualizados se deberían someter a pruebas y verificaciones exhaustivas durante los procesos de desarrollo, incluida la preparación de un programa de actividades detallado y entradas de pruebas y los resultados esperados bajo una variedad de condiciones.

- Las pruebas de aceptación independientes se deberían realizar (tanto para los desarrollos internos y externalizados) para garantizar que el sistema funciona según se espera y sólo como se espera.

- El alcance de las pruebas debería ser en proporción a la importancia y naturaleza del sistema.

8.5 PRUEBAS DE ACEPTACIÓN DE LOS SISTEMAS

- El Encargado de Seguridad de la Información sugerirá criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

- Las pruebas de aceptación del sistema deberán incluir las pruebas de los requisitos de seguridad de la información y la adherencia a las prácticas de desarrollo del sistema seguro.

- Las pruebas también se deberían realizar en los componentes y sistemas integrados recibidos.

- Las pruebas se deberán realizar en un entorno de pruebas realistas para garantizar que el sistema no introducirá vulnerabilidades al entorno de la organización y que las pruebas sean confiables.

8.6 PROTECCIÓN DE LOS DATOS DE PRUEBA

- Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo, que sean tan cercanos como sea posible a los datos reales. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

    - Se debe evitar el uso de bases de datos operativas que contengan información personal. Si se utiliza información de esta índole, esta debe ser despersonalizada antes del uso
    - Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de la autorización.
    - Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

8.7 CONTROL DE CAMBIOS

- Los procedimientos formales de control de cambios se deben documentar y hacer cumplir para minimizar la corrupción de los sistemas de información.

- La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes deben seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

- Este proceso debe incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios.

- Este proceso también debe garantizar que la seguridad y los procesos de control existentes no se exponen a riesgos o peligros, cuando se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

- Previo a cualquier cambio, actualización, o reconfiguración, planificada, en los servidores de aplicaciones, de bases de datos, u otros equipos asociados a la operación de sistemas de información, la jefatura del Área de Desarrollo debe efectuar un análisis y emitir un informe técnico que evalué los impactos y riesgos que puedan generar estos cambios.

8.8 DESARROLLO EXTERNO

- Se debe estandarizar el ciclo de desarrollo de sistemas de acuerdo con lo establecido por la metodología para el Desarrollo y Documentación de Sistemas Informáticos de IND. La metodología puede ser sugerida por el proveedor, pero deberá ser aprobada por IND.

- Se deberá estandarizar los criterios de seguridad y calidad a ser considerados durante cada fase del ciclo de desarrollo de sistemas.

- Los contratos celebrados con empresas de desarrollo externas deberán resguardar la propiedad intelectual, asegurando determinados niveles de confidencialidad de la información manejada en el proyecto.

- Para una adecuada segregación de funciones en la evaluación de cumplimiento de contratos con terceros, el encargado de celebrar y autorizar los mismos no debe ser también el encargado de auditar su cumplimiento.

- Los funcionarios dependientes de IND y personal externo no deberán tener acceso a datos de producción que contengan información reservada sin la adecuada autorización.

- Para propósitos de desarrollo y pruebas, los responsables deberán generar sus propios datos, distintos a los de producción. En caso de ser necesarios se podrá utilizar copias que no contengan información sensible, en caso de ambiente de preproducción se podrán disponer de copias con datos reales.

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 1.0	06-10-2016	Cristian Villalobos Z.	Se elabora primera versión del presente documento.
Versión 2.0	05-12-2018	Cristian Villalobos Z.	Se modifica el formato, la difusión de la política y las responsabilidades.