1. OBJETIVO

Definir los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de información de la organización, de acuerdo a lo establecido en la norma NCh-ISO 27001:2013, y con foco en Ciberseguridad, asegurando la continuidad de los servicios críticos y lograr conservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Todas las actividades desarrolladas para el Instituto Nacional de Deportes (IND) por personal que presta servicios para esta organización y que pertenece a empresas proveedoras de servicios clasificadas como críticas, vinculadas a través del correspondiente contrato de provisión de servicios y que dan soporte a todos los procesos de provisión vigentes en el IND, de acuerdo a lo establecido en la Ficha de Definiciones Estratégicas (A1).

3. MATERIAS ESPECIFICAS QUE ABORDA

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

- A.15.01.01 Política de seguridad de la información para las relaciones con el proveedor.
- A.15.01.02 Abordar la seguridad dentro de los acuerdos con los proveedores
- A.15.01.03 Cadena de suministro de la tecnología de información y comunicación
- A.15.02.01 Monitoreo y revisión de los servicios de proveedor

4. ROLES Y RESPONSABILIDADES

- Encargado/a de Seguridad de la Información:
  - Asesorar al Jefe de Servicio en materias de Seguridad de la Información relacionada con los proveedores.
  - Velar por el cumplimiento de la presente política.

- División de Administración y Finanzas:
  - Gestionar y custodiar los contratos con los proveedores

- Proveedores:
  - Reportar y dar solución a los incidentes relacionados con la disponibilidad de sus servicios para la institución.
  - Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación vinculada al Sistema de Seguridad de la Información.

- Personal externo que presta servicios para el IND:
  - Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación vinculada al Sistema de Seguridad de la Información.

- Usuarios/as:
  - Todo el personal del IND que interactúa con el personal de los proveedores debe dar estricto cumplimiento en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de 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 realizadas en las sesiones del Comité de Seguridad de la Información.

6. DIFUSIÓN

La presente política debe ser difundida por medio de su publicación en la sección “Seguridad de la Información” de la intranet institucional.

7. DEFINICIONES

Proveedor crítico: Es aquel proveedor que, dada la naturaleza del servicio que entregan, tiene acceso a ativos de información e información sensible y/o crítica del IND. Específicamente se consideran proveedores críticos aquellos relacionados con la plataforma básica (comunicaciones y correo electrónico) y de servicios de ciberseguridad (monitoreo, firewall, entre otros).

8. POLÍTICA

8.1 Seguridad de la Información para las relaciones con los proveedores.

Para establecer los controles de seguridad de la información que mitiguen los riesgos asociados al acceso a la información institucional por parte de los proveedores, se debe considerar lo siguiente:

- Identificar y registrar los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los componentes de la infraestructura de TI y a quiénes son autorizados por el IND para acceder a su información.
- Definir para cada proveedor a qué información tiene acceso y los tipos de acceso permitidos.
- Definir los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso.
- Monitorear la adherencia a los requisitos de seguridad de la información establecidos para cada proveedor y tipo de acceso.

8.2 Gestión de incidentes de seguridad

Proveedores de plataforma básica:

Cuando se detecten incidentes relacionados con la disponibilidad de servicios de plataforma básica provistos por terceros, el Gestor de Contrato se debe comunicar con el proveedor para informarlo y solicitar la solución correspondiente, siendo responsabilidad del Encargado de Seguridad la gestión interna de dicho incidente,

Se debe enviar mensualmente un reporte de disponibilidad de servicio al proveedor, indicando el tiempo de interrupción del servicio, lo que permitirá realizar una evaluación anual del comportamiento del proveedor. Dicha evaluación debe ser realizada por el Encargado de Seguridad de la Información.

Proveedores de seguridad:

Los proveedores de seguridad deben reportar incidentes de Ciberseguridad a través del envío de reportes mensuales. Se les debe solicitar un informe mensual de Ciberseguridad a través del cual el Encargado de Seguridad de la Información debe observar si existen incidentes reiterados y, de acuerdo a ello, solicitar al proveedor una solución definitiva al problema, informando a su vez al Encargado de Ciberseguridad. El resultado de estos análisis será un insumo al momento de definir los requisitos de seguridad al renovar los conytratos de servicio

8.3 Prestación de servicios en el IND

Los proveedores solo podrán desarrollar para el IND aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios. De este modo, se entenderá que todas las actividades desarrolladas para el IND por personal perteneciente a empresas proveedoras se encuadran en los contratos de provisión de servicios que vinculan al IND con estos proveedores.

Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizaran de acuerdo a lo establecido en las correspondientes bases y contrato de provisión de servicios.

La empresa proveedora debe proporcionar al IND periódicamente la relación de personas, perfiles, funciones y responsabilidades asociados al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

De acuerdo a lo establecido en las cláusulas asociadas al contrato de provisión de servicios, todo el personal externo que desarrolle labores para el IND deberá cumplir con las directrices definidas en el presente documento y, las políticas y procedimientos del Sistema de Seguridad de la Información del IND. En caso de incumplimiento de cualquiera de estas obligaciones, el IND se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como las sanciones que se consideren pertinentes en relación a la empresa o persona contratada.

La empresa proveedora deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel especifico en las materias correspondientes a la actividad asociada a la prestación del servicio, como de manera transversal

en materia de Seguridad de la Información y Ciberseguridad, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir las Políticas de Seguridad de la Información del IND.

Cualquier tipo de intercambio de información que se produzca entre el IND y las empresas proveedoras se entenderá que ha sido realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

8.4 Confidencialidad de la Información

El personal externo que tenga acceso a información del IND deberá considerar que dicha información, por defecto, tiene carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información del IND a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por el IND.

Queda prohibido para los proveedores revelar, modificar, destruir o hacer mal uso de la información, cualquiera que sea el soporte en que se encuentre contenida.

El proveedor debe resguardar indefinidamente la confidencialidad y no podrá difundir la información a la que tiene acceso, salvo que esté debidamente autorizado por el dueño de ella.

El proveedor debe minimizar el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera de alcance de terceros (ver Política de Pantallas y Escritorios Limpios).

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios tome conocimiento de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación con IND de su empresa. La utilización continuada de la información en cualquier formato o soporte distinta a

la pactada y sin conocimiento del IND, no supondrá en ningún caso una modificación de este punto.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para el IND.

El incumplimiento de estas obligaciones será sancionado en los términos establecidos por las leyes vigentes.

Para garantizar la seguridad de los datos de carácter personal albergados en archivos electrónicos, el personal que pertenece a empresas proveedoras deberá observar las siguientes normas, además de las consideraciones ya mencionadas:

- El personal sólo podrá crear archivos temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos archivos temporales nunca serán ubicados en unidades locales de disco de los PC del personal y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
- No se albergarán datos de carácter personal en las unidades locales de disco de los PC de usuario.
- La salida de soportes informáticos que contengan datos de carácter personal (pendrive, discos duros, CD, computadores, servidores, etc.), fuera de las instalaciones en las que se almacena dicha información, únicamente podrá ser autorizada por el responsable de la información.
- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

8.5 Propiedad intelectual

El personal externo deberá garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

8.6 Intercambio de información

Ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

En relación al intercambio de información dentro del marco del contrato de provisión de servicios, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de archivos a terceras partes no autorizadas de material de la Institución o material que es de alguna u otra manera confidencial.
- Transmisión o recepción de archivos que infrinjan la Ley de Protección de Datos de Carácter Personal o directrices del IND.
- Transmisión o recepción de juegos y/o aplicaciones no relacionadas con las actividades del IND.
- Quienes trabajen en conjunto con el Ministerio del Deportes no deben divulgar información sobre los procesos interno de este.

Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso, cumpliendo con la “Política de Protección de los Datos y Privacidad de la Información Personal”.

Si el tratamiento de datos de carácter personal se llevase a cabo fuera de las instalaciones del IND, dicho tratamiento deberá ser autorizado expresamente por el dueño o responsable del archivo y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de información trata.

La transmisión de datos de carácter personal, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

8.7 Uso apropiado de los recursos

El proveedor se compromete a informar periódicamente al IND de los activos con los que proporciona el servicio contratado.

El proveedor se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo a las condiciones para las que fueron diseñados e implementados.

Los recursos que el IND pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplir con las obligaciones y propósito de la operativa para la que fueron proporcionados. El IND se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Todos los equipos del proveedor que se conectan a la red de producción del IND serán de las marcas y modelos autorizados por el IND. El proveedor pondrá a disposición del IND dichos equipos para que el IND les instale el software homologado y los configure apropiadamente.

Cualquier archivo introducido en la red del IND o en cualquier equipo conectado a ella a través de soporte automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en las Políticas de Seguridad del IND y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

Se deberán restituir al IND todos los activos físicos y destruir o restituir al IND todos los activos de información, sin retraso injustificado, después de la finalización del contrato. Todos los PCs personales a los que el IND les haya instalado software se llevarán al IND para que se formatee el disco duro a la finalización del servicio al IND.

Se prohíbe expresamente:

- El uso de los recursos proporcionados por el IND para actividades no relacionadas con el propósito del servicio.
- La conexión a la red de producción del IND de equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios del IND o bajo supervisión.
- Introducir en los sistemas de información o la red del IND contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en la red del IND cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier

otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo el personal con acceso a la red del IND tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

- Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que el IND les haya asignado.
- Intentar acceder sin autorización explícita a áreas restringidas de los sistemas de información del IND.
- Intentar distorsionar o falsear los registros "log" de los sistemas de información del IND.
- Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos del IND.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos del IND.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de responsabilidad del IND.

8.8 Responsabilidades del usuario

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para el IND respete los siguientes principios básicos dentro de su actividad informática:

- Cada persona con acceso a información del IND es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.
- Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
- Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.

Cualquier persona con acceso a información de responsabilidad del IND deberá seguir las siguientes directivas en relación a la gestión de las contraseñas:

- Seleccionar contraseñas robustas.
- Pedir cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar antiguas contraseñas.
- Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión.
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.

Cualquier persona con acceso a información de responsabilidad del IND deberá velar para que los equipos queden protegidos cuando vayan a quedar desentendidos (ver Política de Pantallas y Escritorios Limpios).

Cualquier persona con acceso a información de responsabilidad del IND deberá respetar al menos las siguientes Políticas de Escritorio Limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo (ver Política de Pantallas y Escritorios Limpios):

- Almacenar bajo llave documentos en papel y los medios informáticos con información de responsabilidad del IND en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- No dejar desatendidos los equipos asignados a funciones críticas del IND, y bloquear su acceso cuando sea estrictamente necesario.
- Proteger, siempre que se utilice información de responsabilidad del IND, tanto los puntos de recepción y envío de información (correo postal, scanner) como los equipos de duplicado (fotocopias, scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad del usuario.
- Retirar, sin retraso injustificado, cualquier información confidencial responsabilidad del IND, una vez impresa.
- Los listados con datos de carácter personal o información confidencial responsabilidad del IND deberán almacenarse en un lugar seguro al que únicamente tengan acceso personal debidamente autorizado.

- Los listados de datos de carácter personal o información confidencial responsabilidad del IND deberán eliminarse de manera segura una vez que ya no sean necesarios.
- Las personas con acceso a sistemas y/o información del IND no deben, sin autorización expresa, realizar pruebas para detectar y/o utilizar una supuesta debilidad o incidente de seguridad, en caso de identificarse incidentes o debilidades que puedan suponerse relacionadas con la seguridad de la información.
- Ninguna persona con acceso a sistemas y/o información del IND intentará, sin autorización expresa, por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditorías expresamente autorizadas.
- Ningún dato de carácter personal de responsabilidad del IND serán almacenado en equipos de usuario personales ni soporte de información personal.

Todo personal que acceda a la información y/o los sistemas de responsabilidad del IND deberá seguir normas de actuación:

- Proteger la información confidencial perteneciente o cedida por terceros a IND de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
- Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- Contar con la autorización necesaria para obtener el acceso a los sistemas de información.
- Conocer, aceptar y cumplir las presentes políticas antes de acceder a la información y/o los sistemas del IND.

8.9 Equipo de usuario

Los proveedores de servicios deberán asegurarse de que todo el equipamiento informático del usuario que sea utilizado para acceder a la información de responsabilidad del IND cumpla las siguientes normas:

- Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo.

- Ningún equipo de usuario dispondrá de herramientas que puedan transgredir el sistema de seguridad ni las autorizaciones dentro de los sistemas de la institución.
- Los equipos de usuario se mantienen de acuerdo a las especificaciones de los fabricantes.
- Todos los equipos de usuario están adecuadamente protegidos frente a malware (virus informáticos):
    - El software antivirus se deberá instalar y usar en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
    - Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
    - El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los archivos de definición de virus.

Se velará especialmente por la seguridad de todos los equipos móviles de usuario que contengan información de responsabilidad del IND o permitan acceder a ella de algún modo, mediante las siguientes acciones:

- Verificando que no incluyan más información de responsabilidad del IND que la que sea estrictamente necesaria.
- Garantizando que se aplican controles de acceso a dicha información.
- Minimizando los accesos a dicha información en presencia de personas ajenas al servicio provisto por el IND.
- Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a golpes.
- Tomando especiales preocupaciones en el exterior de las dependencias del IND para evitar la visión accidental por parte de terceras personas de la información de responsabilidad del IND.

8.10 Gestión de equipamiento “hardware”

Los proveedores de servicios deberán asegurarse de que todos los equipos proporcionados por el IND para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberán cumplir con lo siguiente:

- El proveedor deberá mantener una relación actualizada de equipos proporcionados por el IND y usuarios de dichos activos, o responsables asociados en caso de que los

activos no sean de uso unipersonal. Dicha relación podrá ser requerida por el IND en cualquier momento.

- Siempre que un proveedor quiera reasignar algún equipo del IND que haya contenido información de responsabilidad del IND deberá devolver temporalmente al IND dicho activo para que se puedan llevar a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación.
- En caso de que un proveedor cese en la prestación del servicio, deberá devolver al IND toda la relación de equipos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios. Sólo en el caso de activos de información el proveedor podrá proceder a su eliminación segura, en cuyo caso deberá notificar al IND dicha eliminación.

8.11 Cadena de suministro de la tecnología de información y comunicación

Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones, considerando lo siguiente:

- Requisitos para la adquisición de tecnologías, productos o servicios de información y comunicación.
- Requisitos en caso de subcontratación para partes del servicio de tecnología de información y comunicación proporcionados al IND.
- Establecer garantías para el funcionamiento de los productos o servicios provistos, de acuerdo a lo esperado.

8.12 Monitoreo y revisión de los servicios

Con el objetivo de mantener un adecuado nivel de seguridad de la información en los servicios o productos provistos al IND, se debe realizar un monitoreo periódico a los proveedores críticos. El ESI deberá, al menos una vez al año, realizar una revisión y evaluación de los servicios entregados por los proveedores críticos. Para ello se deberá realizar una auditoría in situ al proveedor y hacer una revisión de los incidentes ocurridos durante el año que tengan relación con el servicio o producto suministrado al IND por dicho proveedor.

Dicha revisión será un insumo para las decisiones que se deben tomar respecto de la continuidad de los servicios del proveedor o de las acciones de mejora si corresponde.

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 0.0	06-04-2017	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 las responsabilidades.
Versión 2.0	16-05-2019	Cristian Villalobos Z.	Se detalla la forma en que los proveedores participan de la gestión de los incidentes de seguridad en los cuales se ven directamente involucrados y se incorporan los controles normativos 15.1.3 y 15.2.1