POLÍTICA DE SEGURIDAD DE INFORMACIÓN Y TRATAMIENTO DE DATOS PERSONALES

I.- CONTEXTO

La Corporación Instituto Nacional del Fútbol, Deporte y Actividad Física (INAF), reconoce que la información es un recurso valioso que, bien gestionada, impacta positivamente la toma de decisiones. Concibe el gobierno de datos como una manera coherente de organizar a colaboradores, procesos y sistemas. La adecuada gestión del conocimiento y la información generada, permite mejorar el cumplimiento de los propósitos institucionales en todos sus ámbitos de acción, en especial en los procesos esenciales: formación, investigación y vinculación con el medio.

Esta política gobierna un sistema integral de seguridad compuesto por otras normativas, por la definición de responsables, por un plan de ciberseguridad y por procesos que sustentan su operación. Entrega lineamientos generales y una estructura de gestión cuyo objetivo permitirá garantizar la seguridad de la información y de los datos personales tanto antes como durante su tratamiento, conforme a lo estipulado en la legislación vigente. Además, busca facilitar su aprovechamiento en una lógica organizacional de toma de decisiones basada en evidencias. Y por consiguiente, establece las pautas en los ámbitos de seguridad y tratamiento de la información y de los datos personales, sin perjuicio que en el futuro se confeccionen otras normativas en esta materia.

II.- ÁMBITO DE APLICACIÓN

Esta normativa tiene un alcance general y será aplicable a todos los activos de información utilizados y generados por la Corporación Instituto Nacional del Fútbol, Deporte y Actividad Física. Abarcará a todas aquellas personas de la comunidad institucional que participen directa o indirectamente en la tenencia, tratamiento o generación de información, así como a terceros o personal externo vinculados por relación contractual con la Corporación.

III. – OBJETIVOS

La Corporación Instituto Nacional Del Fútbol, Deporte y Actividad Física establece los siguientes objetivos en materia de seguridad de la información, ciberseguridad y protección de la infraestructura relacionada:

- Contar con normativas que regulen la actividad interna en materia de seguridad y tratamiento de información, conforme a los propósitos institucionales y a las exigencias contenidas en la legislación vigente.
- Gestionar el cambio cultural para asegurar que todas las actividades de enseñanza, investigación, operación y administración consideren la seguridad de la información, la ciberseguridad y la protección de la infraestructura relacionada. Esto incluye definir a las responsabilidades en la gestión y tratamiento de los datos a lo largo de la Corporación y comunicar y capacitar respecto a seguridad de la información y ciberseguridad.
- Diseñar nuevos procesos y adecuar algunos existentes, para identificar, gestionar y mitigar los riesgos de la información y de los activos de infraestructura.
- Contar con infraestructura tecnológica y sistemas seguros a los cuales acceden los usuarios autorizados para llevar a cabo sus funciones equilibrando adecuadamente la usabilidad y la seguridad.
- Cumplir con la normativa vigente: LEY SOBRE PROTECCIÓN A LA VIDA PRIVADA N° 19.628 y normativas afines.
- Gestionar y resolver los incidentes de manera efectiva y aprender de ellos para mejorar el entorno de seguridad de la Corporación.

IV.- LINEAMIENTOS GENERALES PARA LA SEGURIDAD DE LA INFORMACIÓN Y DE LOS DATOS PERSONALES

En la Corporación Instituto Nacional Del Fútbol, Deporte y Actividad Física los datos personales serán protegidos, previo a y durante su tratamiento y transferencia, según lo dispuesto en el artículo 19 Nº4 de la Constitución Política de la República y lo preceptuado en la Ley Nº19.628, sobre Protección de la Vida Privada. Para lo cual, y con la finalidad de resguardar la información y los datos personales, la Corporación organizará su trabajo en torno a cuatro ejes, siendo éstos la institucionalidad, los procesos, la seguridad de los sistemas y la cultura organizacional. La institucionalidad contemplará principalmente las normativas internas y la definición de responsables, mientras que el eje procesos considerará, entre otros, el proceso de gestión de los accesos, la clasificación de los datos y el proceso de tratamiento de datos. Por su parte, la seguridad de los sistemas contemplará

un plan de ciberseguridad y un protocolo frente a ataques informáticos y hackeos, entre otros. Por último, el eje cultura organización comprenderá principalmente el plan de comunicación, el plan de capacitación y el monitoreo de las prácticas de seguridad.

Los lineamientos generales respecto a la seguridad de la información y de los datos personales, siendo esta normativa interna no taxativa, son los siguientes:

A) Responsabilidades hacia los Titulares de Datos

La Corporación se compromete a resguardar los datos personales de los titulares de datos y responder ante el ejercicio de sus derechos, siendo éstos, el acceso, la cancelación, la rectificación y la oposición.

B) Clasificación de la Información

La información, incluido los datos personales, se clasifica a partir de su valor y sensibilidad para la Corporación y conforme a lo establecido por la normativa vigente. Para esto la Corporación Instituto Nacional Del Fútbol, Deporte y Actividad Física se compromete a elaborar un instructivo con una clasificación de información según el grado de protección que se le quiera dar, instructivo que contendrá una definición de cada una de las categorías.

C) Ciberseguridad

La Corporación Instituto Nacional Del Fútbol, Deporte y Actividad Física asume el deber de evitar la pérdida, los daños, el robo y el compromiso de sus activos de información. Para ello contará con un plan de ciberseguridad que contemplará medidas técnicas y organizativas para el resguardo de la infraestructura, de la información y de los datos personales en particular, conforme a su clasificación. Ante la ocurrencia de incidentes se activará un plan efectivo para reducir su impacto.

D) Procedimientos para el resguardo de la información y de los datos personales

Existirán mecanismos para mantener la seguridad de la información que la Corporación quiera proteger y de los datos personales que por ley se deben proteger, gestionando los accesos a los sistemas y los permisos para tratar datos, e implementando medidas de seguridad que impactan los sistemas y la cultura.

E) Roles y Responsables de la Seguridad de la Información y de los Datos Personales

Para el cumplimiento de esta política, la Corporación define que el Responsable de Datos es la Corporación Instituto Nacional del Fútbol, Deporte y Actividad Física. Complementariamente a la responsabilidad legal, la responsabilidad sobre la información y los datos personales está distribuida a lo largo de la Institución, siendo responsables los siguientes cargos, roles e instancias:

- Encargado de Datos: este rol tiene entre sus responsabilidades el liderar la ejecución de esta política y responder ante el ejercicio de los derechos de los titulares de datos, autorizar a tratar datos a personas sin autorización para ello y presidir el Comité de Seguridad.
- Comité de Seguridad: es responsable de desarrollar las normativas asociadas a la seguridad de la información y de los datos personales, velar, una vez ya implementadas, por el adecuado cumplimiento de la política de seguridad de información y tratamiento de datos personales en el ámbito de la ciberseguridad, de hacer el seguimiento al cumplimiento del plan de ciberseguridad y del trabajo organizado en torno a los 4 ejes, siendo estos, institucionalidad, procesos, seguridad de los sistemas y cultura. Será un órgano consultivo del Encargado de Datos y estará integrado, además de éste último, por el Vicerrector Académico, el Vicerrector de Administración y Finanzas y por el Jefe de Control de Gestión e Información.
- Autoridades de la Corporación: los miembros del Comité Directivo Superior, los directores y jefes de unidades transversales, son responsables del cumplimiento de esta política y de los datos personales en el/las área/s que gobiernan.
- Personas autorizadas a acceder a información sujeta a protección: son responsables de cumplir con lo establecido en la presente política y normativa vigente y leyes afines en su caso, también respecto de normativas relativas a la seguridad y tratamiento de la información, dictadas en su oportunidad por la Corporación.

F) Datos Reportados a Externos y Cesión de Datos

En el reporte de información que la Corporación Instituto Nacional del Fútbol debe realizar periódicamente a organizaciones gubernamentales asociadas al Ministerio de Educación, u otras, actuará cumpliendo la legislación vigente en materia de protección de los datos personales, la ley de Educación Superior y cualquier otra regulación que sea aplicable.

En la cesión de datos a otros Responsables de Datos, distintos a las organizaciones gubernamentales antes mencionadas, la Corporación se compromete a realizarla sólo si cuenta con el consentimiento del Titular de Datos y en los casos de excepción señalados por la ley.

G) Transferencia Internacional de Datos Personales

La Corporación Instituto Nacional del Fútbol realizará transferencia internacional de datos personales siempre amparada en documentos jurídicos entre quien entrega y quien recibe, que establecen derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control.

V.- LINEAMIENTOS GENERALES PARA EL TRATAMIENTO DE LA INFORMACIÓN Y DE LOS DATOS PERSONALES

La Corporación Instituto Nacional del Fútbol realizará el tratamiento de la información en base a las mejores prácticas de seguridad y a los controles mínimos que deben ser aplicados.

Por su parte, el tratamiento de datos personales se realizará conforme a la evaluación de los riesgos y los niveles de seguridad requeridos, acorde a lo estipulado según la ley vigente, tanto antes como durante el tratamiento.

Para llevar a cabo el tratamiento de datos personales, la Corporación Instituto Nacional del Fútbol se basará en los siguientes lineamientos generales, siendo esta normativa interna no taxativa:

A) Principios del Tratamiento de Datos Personales

El tratamiento de los datos personales en la Corporación Instituto Nacional del Fútbol se regirá por los siguientes principios entre los cuales están:

- Licitud: los datos personales sólo se tratarán conforme a lo establecido en la ley.
- Finalidad: los datos personales deberán ser recolectados para fines específicos, explícitos y lícitos y serán tratados conforme a estos fines.
- Proporcionalidad: el tratamiento de los datos personales se limitará a lo que resulte necesario respecto a los fines definidos y cuya conservación se definirá en atención a la legislación vigente.
- Calidad: los datos personales deben ser exactos, completos, actuales y en relación a los fines del tratamiento.
- Confidencialidad: el responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos, deber que subsiste aún después de terminada la relación con el titular de los datos.

Para que el tratamiento de datos personales sea lícito, se deberá contar con el consentimiento del titular de datos, salvo determinadas causales estipuladas por la ley vigente. El consentimiento deberá contemplar los fines específicos para los cuales se realizará el tratamiento.

B) Procesos para el Tratamiento de los Datos

La Corporación dispondrá de procesos internos para realizar el tratamiento de datos buscando equilibrar la seguridad con la usabilidad y cumplir con las exigencias de la legislación vigente. Estos procesos se complementarán con normativas, la definición de responsables, las medidas de ciberseguridad, mecanismos de control, indicadores de cumplimiento y las acciones necesarias para gestionar el cambio cultural.

Entre los procesos definidos estarán el de otorgamiento y eliminación de los accesos y los de descarga, modificación y uso de datos.

C) Deberes a cumplir en el Tratamiento de Datos Personales

Aquéllos que traten los datos personales contenidos en las bases de datos de la Corporación, deberán cumplir con los siguientes deberes según la normativa vigente:

- Cumplir con lo estipulado en las políticas y otras normativas que la Corporación tenga respecto al tratamiento de la información y de los datos personales.
- Cumplir con la confidencialidad de los datos personales que conciernan a un titular, salvo cuando el titular los hubiere hecho manifiestamente públicos.
- Aplicar las medidas técnicas y organizativas apropiadas con anterioridad y durante el tratamiento de datos, con el fin de cumplir los principios del tratamiento de datos y proteger los derechos del titular establecidos en la ley.
- Adoptar las medidas de seguridad necesarias para el adecuado resguardo de los datos personales y evitar su pérdida, filtración, daño accidental y destrucción.
- Reportar vulneraciones a las medidas de seguridad al Encargado de Datos designado por la Corporación.
- Cancelar o devolver, a quien corresponda, los datos tratados.

La Corporación adoptará todas las medidas tendientes a capacitar a los colaboradores que tengan acceso a datos personales acerca de la forma correcta de ejercer sus tareas asociadas al uso de datos personales, facilitando el íntegro cumplimiento de la normativa legal.

VI.– GLOSARIO DE TÉRMINOS

A continuación, se definen conceptos relativos a la seguridad de la información y su tratamiento de datos personales en el marco del contenido de esta política.

A. Activo de Información: son los datos creados o utilizados por un proceso de la institución bajo cualquier medio, digital, papel u otros; hardware y software utilizado para el procesamiento, transporte o almacenamiento de información; personas que manejen datos o un conocimiento específico importante. “Es algo que una organización valora y por lo tanto debe proteger”.
B. Seguridad de la Información: es el conjunto de mecanismos utilizados para gestionar los procesos, herramientas y políticas necesarias para prevenir, detectar, documentar y contrarrestar las amenazas a la información digital y no digital.
C. Confidencialidad: propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

D. Integridad: la integridad de la información se refiere a la exactitud y consistencia general de los datos o, expresado de otra forma, como la ausencia de alteración cuando se realiza cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios.
E. Autenticidad: la autenticidad es la seguridad de que un mensaje, una transacción u otro intercambio de información, proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad.
F. Disponibilidad: se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.
G. Titular de Datos: persona natural a la que se refieren los datos de carácter personal.
H. Datos Personales: datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
I. Datos Personales Sensibles: aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
J. Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma los datos personales o conjuntos de datos personales.
K. Cesión de datos: es la transferencia de datos personales por parte del responsable de datos a otro responsable de datos.
L. Responsable de datos: persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal, de conformidad con lo dispuesto en la Ley N°19.628, sobre Protección de la Vida Privada.
M. Encargado de datos: responsable institucional en la gestión de los datos y la ejecución de esta política.
N. Incidente de seguridad de la información: cualquier ocurrencia no deseada identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
O. Ciberseguridad: es la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

Santiago, octubre de 2019.