ANEXO A LA RESOLUCIÓN N°2025000448 DE 16/05/2025 DOCUMENTO POLÍTICA GENERAL PARA LA SEGURIDAD DE LA INFORMACIÓN, LA SEGURIDAD DIGITAL, LA CIBERSEGURIDAD Y LA PROTECCIÓN DE LA PRIVACIDAD DE LOS DATOS PERSONALES DE INDEPORTES ANTIOQUIA, DEFINIENDO LINEAMIENTOS DE PRINCIPIOS, ALCANCE, ROLES Y RESPONSABILIDADES, APLICABILIDAD Y CUMPLIMIENTO.

Contenido

INDEPORTES ANTIOQUIA, con NIT 811.007.127-0, es una entidad responsable con la privacidad y seguridad digital y, entiende la importancia de la adecuada gestión de los activos de información y el cuidado de los datos personales de usuarios internos, externos y partes interesadas, por lo tanto, El gerente y el Comité de Gestión y Desempeño de INDEPORTES ÁNTIOQUIA, establecen la Política General para la Seguridad de la Información, la Seguridad Digital, la Ciberseguridad y la Protección de la Privacidad, definiendo lineamientos de principios, alcance, roles y responsabilidades, aplicabilidad y cumplimiento.

OBJETO: Formular, implementar y promover la aplicación de mejores prácticas enfocadas a la seguridad digital, protección de la privacidad de los datos personales y la seguridad de la información de INDEPORTES ANTIOQUIA, que estén alineadas al cumplimiento regulatorio, al estándar ISO 27001 y a la normatividad asociada, con el fin de elevar los niveles de confianza en la información y los datos personales manejados por el Instituto, fomentando una cultura organizacional orientada a la seguridad digital y ciberseguridad, reduciendo los riesgos previamente identificados, preservando los activos de información y fortaleciendo aspectos clave como la integridad, la confidencialidad y la disponibilidad.

TÉRMINOS Y DEFINICIONES.

- Política general de seguridad de la información: Es el documento base en el que la alta gerencia se compromete a proteger los activos de información y los datos institucionales estableciendo lineamientos. Esta política es el componente base para la puesta en marcha del modelo de seguridad y privacidad de la información y es el requisito principal de la norma ISO 27001 para el sistema de gestión de seguridad de la Información, esta debe contener objetivo, aplicabilidad, alcance, principios, nivel de cumplimiento, fundamentos, roles y responsabilidades.
- Manual de políticas de la seguridad de la información: Conjunto de controles en donde se especifican una a una las políticas de la seguridad de la información, basadas en los principios que se acordaron en la política general de seguridad de la información.
- Sistema de gestión de la seguridad de la información (SGSI): Es un proceso sistémico, documentado, conocido por toda la entidad, que busca preservar la confidencialidad, integridad y disponibilidad de la información. Bajo el anterior concepto se fundamenta la norma ISO-IEC 27001 en particular y otros estándares en general, basados en la implementación de una serie de políticas y controles para administrar la seguridad de la información.
- Modelo de seguridad y privacidad de la información: Modelo base para la Implementación del Sistema de Gestión de la Seguridad de la Información. El Ministerio de las TIC en su decreto único sectorial 1078 de 2015, determina que las entidades públicas deben implementar la estrategia de Gobierno Digital, y presenta una serie de guías para establecer dicho modelo.
- Confidencialidad: Condición que asegura que la información solo sea accesible por personas o sistemas autorizados, evitando divulgaciones no permitidas.
- Integridad: Propiedad que garantiza que la información se mantenga completa, exacta y protegida contra modificaciones no autorizadas, asegurando que sus valores y atributos originales no sean alterados de manera indebida.

- Disponibilidad: Característica que asegura que los datos y sistemas de información estén accesibles y utilizables por los usuarios autorizados en el momento en que lo requieran, minimizando interrupciones o fallas.
- Seguridad de la Información: Conjunto de prácticas y medidas diseñadas para preservar la confidencialidad, integridad y disponibilidad de la información física y lógica, protegiéndola contra amenazas como el acceso no autorizado, alteraciones o destrucción.

- Seguridad Digital: Estrategias y soluciones que integran tecnologías, políticas y buenas prácticas para proteger la información digital y los sistemas electrónicos, incluyendo tanto dispositivos personales como infraestructuras organizacionales.
- Ciberseguridad: Disciplina que se enfoca en proteger los sistemas informáticos, redes, software y datos que viajan por internet, ante ataques maliciosos, fraudes electrónicos y otras vulnerabilidades que comprometan la infraestructura digital.
- Aviso de Privacidad: Documento que informa al titular sobre las políticas de tratamiento de datos personales de la entidad, entregado al momento de la recolección. Este incluye información sobre el responsable del tratamiento, derechos del titular y los canales para acceder a las políticas.
- Base de Datos: Colección sistemática de información personal organizada para facilitar su uso y manejo, orientada a contextos específicos.
- Datos Personales: Cualquier información relacionada con una persona natural identificada o identificable. Pueden clasificarse como datos públicos, privados, sensibles o semiprivados.
- Dato Privado: Información perteneciente a la esfera íntima de una persona, cuyo acceso está limitado y protegido, solo accesible mediante autorización expresa o por orden judicial.
- Dato Público: Información que no tiene carácter reservado ni privado, como datos relacionados con el estado civil o documentos públicos y judiciales sin restricciones.
- Dato Semiprivado: Información que no es pública ni íntima, pero puede ser de interés para un sector, como datos financieros o comerciales.
- Datos Sensibles: Información que, por su naturaleza, puede impactar la privacidad del titular o generar riesgos de discriminación. Ejemplos incluyen datos biométricos, de salud, creencias religiosas o políticas.
- Datos Abiertos: datos públicos que están almacenados en formato estándar, generalmente sin estar procesados, para poder ser reusados al servicio de la ciudadanía.
- Información pública reservada: Es la información pública con excepciones amparadas por la ley de protección de datos personales.
- Información pública Clasificada: Según el Departamento Administrativo de la Función Pública, es aquella información que estando en poder de un sujeto responsable en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en la ley.
- Almacenamiento de Información: Proceso de preservar datos físicos o digitales en sistemas que garantizan medidas de protección adecuadas. Esto incluye controles físicos, tecnológicos y ambientales en áreas restringidas, tanto en instalaciones propias como en centros gestionados por terceros.
- Autorizaciones: Manifestación libre y consciente del titular de los datos, otorgada previa y expresamente, para la inclusión de su información en una base de datos. Este consentimiento debe informar claramente los datos a recolectar y las finalidades de su uso.
- Contratos de Transmisión de Datos: Acuerdo entre el responsable y el encargado del tratamiento de datos, que establece las tareas y obligaciones de cada parte en relación con el tratamiento de la información.
- Derechos de los Niños, Niñas y Adolescentes: Los datos de menores deben ser tratados bajo estrictos criterios de protección, considerando su bienestar y los derechos prevalentes establecidos en la normativa.
- Encargado del Tratamiento: Persona o entidad que, por mandato del responsable, realiza las operaciones necesarias para la administración de los datos personales.

- Información: Conjunto estructurado de datos transformados en un mensaje útil para un fin específico, almacenados en medios físicos o digitales.
- Información Digital: Datos procesados o transmitidos mediante plataformas electrónicas y digitales, como correos electrónicos o sistemas informáticos.
- Información Pública: Información generada o controlada por entidades públicas, disponible para acceso ciudadano, salvo excepciones previstas por la ley.
- Información Pública Clasificada: Datos en poder de entidades públicas cuyo acceso está restringido debido a su naturaleza privada o semiprivada, bajo justificaciones legales.
- Información Pública Reservada: Información pública que se restringe por razones de interés colectivo o público, conforme a las disposiciones legales aplicables.
- Responsable del Tratamiento: Persona o entidad con poder de decisión sobre el uso y gestión de bases de datos, encargada de definir los objetivos y garantizar el cumplimiento de las normativas.
- Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- Titular de los Datos: Persona natural cuyos datos personales son objeto de tratamiento por parte de la entidad.
- Tratamiento de Datos: Operaciones realizadas sobre información personal, como su recolección, almacenamiento, uso, distribución o eliminación, conforme a su propósito.
- Transferencia: Proceso en el cual el responsable de los datos transfiere la información a otra entidad, dentro o fuera del país, bajo condiciones que cumplen con la normativa.
- Terceros: Entes externos interesados en acceder a datos personales, tales como ciudadanos, organismos de control o certificación.
- Anonimización: Técnica que transforma datos personales en información no vinculable a una persona específica, asegurando que no puedan ser asociados razonablemente al titular.

APLICABILIDAD: La Política General para la Seguridad de la Información, la Seguridad Digital, la Ciberseguridad y la Protección de la Privacidad de los Datos Personales de INDEPORTES ANTIOQUIA, aplica para todos los usuarios y las partes interesadas del Instituto. (Organismos deportivos, Entes Deportivos Municipales, funcionarios, contratistas, entidades gubernamentales y no gubernamentales, proveedores, ciudadanía, medios de comunicación y Atletas y Paraatletas).

ALCANCE: La Política General para la Seguridad de la Información, la Seguridad Digital, la Ciberseguridad y la Protección de la Privacidad de los Datos Personales de INDEPORTES ANTIOQUIA, cubre todos los procesos y dependencias de la entidad y se fundamenta en el modelo de seguridad y privacidad de la información sugerido por el Ministerio de las TIC y los requisitos de la norma ISO 27001, teniendo como base los siguientes principios detallados a continuación:

PRINCIPIOS: Los principios de la política general de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales de INDEPORTES ANTIOQUIA, están basados en el modelo de seguridad del Ministerio de las TIC, la práctica de gestión de riesgos del Departamento Administrativo de la función pública y los objetivos de control de la norma ISO/IEC 27002.

a) **Principio sobre las instalaciones**: Proteger la infraestructura tecnológica y activos críticos que soportan la información generada, procesada o resguardada por los procesos de la institución, gestionando el riesgo que se genera de los accesos otorgados a terceros (los clientes internos, externos y partes interesadas).
b) **Principio sobre la información**: Proteger los datos y la información creada, procesada, transmitida o resguardada por los procesos de la institución, con el fin de minimizar impactos

financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles y procedimientos de acuerdo con la clasificación de la información de su propiedad o en custodia.

c) **Principio sobre el tratamiento de datos personales de Niños Niñas y Adolescentes**: INDEPORTES ANTIOQUIA se compromete a cumplir rigurosamente los principios establecidos en el artículo 4 de la Ley 1581 de 2012; Esto incluye la adopción de procedimientos y medidas claras y efectivas que garanticen que los datos sean manejados de manera responsable, ética y conforme a los derechos fundamentales de los titulares.
d) **Principio sobre el personal**: Proteger la información de las amenazas originadas por parte del personal de la institución, usuarios y partes interesadas.
e) **Principio sobre las aplicaciones**: Controlar la operación de sus procesos institucionales garantizando la seguridad de los recursos tecnológicos relacionados con el software, su ciclo de vida y su debido licenciamiento.
f) **Principio sobre las comunicaciones**: Fortalecer la cultura de la seguridad digital en los funcionarios, terceros, aprendices, practicantes y clientes con estrategias de sensibilización de la protección de la información y los datos personales.
g) **Principio sobre los procesos**: Garantizar la disponibilidad de sus procesos institucionales y la continuidad de la operación basada en el impacto que pueden generar los eventos.
h) **Principio sobre los sistemas operativos**: Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas, teniendo en cuenta el licenciamiento vigente.
i) **Principio sobre los datos personales**: En particular, la INDEPORTES ANTIOQUIA garantiza la *legalidad* en el tratamiento de los datos personales, cumpliendo con todas las disposiciones normativas aplicables y asegurando que cada proceso de recolección, almacenamiento, uso y supresión sea debidamente autorizado por los representantes legales de los niños niñas y adolescentes a través del consentimiento informado.

   Se garantiza igualmente la *finalidad*, asegurando que los datos personales solo sean tratados para propósitos específicos, legítimos y previamente informados a los titulares, estos datos usarán en fines institucionales que promuevan su desarrollo integral, específicamente para inscripción y participación en actividades deportivas y recreativas, medicina deportiva, seguimiento y evaluación de programas deportivos, comunicaciones relacionadas con las actividades organizadas por INDEPORTES ANTIOQUIA.

   Asimismo, INDEPORTES ANTIOQUIA asegura el cumplimiento de principios como la *veracidad o calidad* de la información, evitando el manejo de datos incompletos o inexactos, y la *transparencia,* permitiendo que los representantes legales accedan fácilmente a información sobre el tratamiento de los datos. Además, la entidad se compromete a garantizar la *confidencialidad,* evitando el acceso no autorizado a los datos personales y adoptando las medidas necesarias para proteger de manera estricta la privacidad de los niños, niñas y adolescentes.

   Lo representantes legales de los niños, niñas y adolescentes pueden conocer, actualizar y rectificar sus datos personales, solicitar prueba de la autorización otorgada, ser informados respecto al uso de sus datos personales, presentar solicitudes, peticiones, quejas o reclamos respectivos ante la institución o ante la superintendencia de industria y comercio en caso de incumplimiento.

DIRECTRICES DE PRIVACIDAD PARA EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES:

El artículo 15 de La Constitución Política, La ley 1266 de 2008 (Habeas Data), la ley 1581 de 2012 (protección de datos personales) y la ley 1712 de 2014 (clasificación de la información) y demás regulaciones orientadas a la protección y tratamiento de los datos personales y la información, establecen

una serie de parámetros en los que INDEPORTES ANTIOQUIA define a continuación según los principios y naturaleza de la Ley que nos acoge:

Principios para el tratamiento de datos personales (ley 1581 de 2012)

1. *Principio de legalidad en materia de tratamiento de datos:* El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.
2. *Principio de finalidad:* INDEPORTES ANTIOQUIA aplica este principio de acuerdo con la constitución y la ley, en donde se informa al titular la finalidad del tratamiento del dato, el cual va enfocado a fines institucionales que promuevan su desarrollo integral, específicamente para inscripción y participación en actividades deportivas y recreativas, medicina deportiva, seguimiento y evaluación de programas deportivos, comunicaciones relacionadas con las actividades organizadas por la institución.
3. *Principio de libertad:* El tratamiento de datos personales solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
4. *Principio de veracidad o calidad:* La información personal sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, en este sentido, se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
5. *Principio de transparencia:* En el tratamiento de datos personales debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
6. *Principio de acceso y circulación restringida:* El tratamiento de datos personales está sujeto a los límites que se derivan de la naturaleza de los mismos, de las disposiciones de ley y la constitución. En este sentido, su tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en ley. En este sentido, los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la ley.
7. *Principio de seguridad:* La información personal sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas a través de procedimientos y mejores prácticas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. INDEPORTES ANTIOQUIA con esta política y la formulación e implementación de un modelo de Seguridad de la Información, la Seguridad Digital, la Ciberseguridad y la Protección de la Privacidad de los Datos Personales, basado en los lineamientos del Ministerio de Tecnología y las Comunicaciones-Mintic, el estándar ISO 27001 y el sistema de gestión de calidad de la institución, se compromete a establecer una mejora continua para la protección de los datos personales y en general de la seguridad de la información.
8. *Principio de confidencialidad:* Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

Identificación y contacto del encargado del manejo y tratamiento de los datos y bases de datos:

NOMBRE O RAZÓN SOCIAL	INDEPORTES ANTIOQUIA
DIRECCIÓN:	Carrera 48 # 70-180
CIUDAD DE DOMICILIO:	Medellín- Antioquia
TELÉFONO DE CONTACTO	+57 604 520 08 90
CORREO ELECTRÓNICO:	contactenos@indeportesantioquia.gov.co
PQRSD POR LA WEB	https://www.indeportesantioquia.gov.co

Autorización del titular para el tratamiento de sus datos:

Para cualquier información que sea suministrada por el titular por medio de diligenciamiento de formularios y formatos, se requerirá autorización previa para el tratamiento de datos del titular a excepción de los siguientes casos:

• Información requerida por la Superintendencia Financiera de Colombia, Organismos de Control del Estado, en ejercicio de sus funciones legales o una orden judicial.

• Datos de naturaleza pública.

• Casos de urgencia médica o sanitaria.

• Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

• Datos relacionados con el Registro Civil de las Personas.

Finalidad de los datos tratados por INDEPORTES ANTIOQUIA:

La institución recolectará, procesará, almacenará, usará y custodiará de forma segura, los datos personales ya sea manual o sistematizado para lo siguiente, de acuerdo con los estipulado en la Ley 1581 de 2012 y los Decretos 1377 de 2013 y 1759 de 2016.

- Datos personales relacionados con las actividades propias de los procesos y misionalidad de INDEPORTES ANTIOQUIA las cuales son: apoyo técnico, científico y psicosocial, acompañamiento institucional, actividad física, recreación, servicio al ciudadano, juegos deportivos institucionales, deporte, y capacitación para organizaciones deportivas.
- Responder a PQRSD realizada por los titulares o entes de control.
- Finalidades propias para el cumplimiento regulatorio y obligaciones legales o jurídicas.

Tratamiento de datos sensibles:

INDEPORTES ANTIOQUIA con previa autorización del titular tratará los siguientes tipos de datos sensibles:

- Historias ocupacionales
- Historias clínicas
- Datos raciales y/o de origen étnico.
- Datos biométricos.
- Datos relacionados con la orientación sexual.

- Datos pertenecientes a organizaciones sociales.
- Información general de personas que los pueda poner en riesgo.

Se prohíbe el tratamiento del dato sensible excepto salvo cuando:

- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.
- El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización

Tratamiento de datos privados:

INDEPORTES ANTIOQUIA con previa autorización del titular tratará los siguientes tipos de datos privados según sea el caso:

- Número de documento de identidad
- Número de Pasaporte
- Fecha de Nacimiento
- Estado Civil
- Numero de cuentas bancarias.
- Correo electrónico.
- Números telefónicos
- Fotos y videos tomadas desde dispositivo móvil propio.
- Fotos y videos donde aparezca el titular.
- Género.

Tratamiento de datos semiprivados:

Estos a pesar de que no tienen naturaleza pública, ni reservada, ni sensible, INDEPORTES ANTIOQUIA solo puede dar a conocer o divulgar estos datos cuando el titular dio su autorización para tratar o dar a conocer esto a terceros, los cuales son:

- Medios audiovisuales
- Imágenes
- Datos financieros.
- Datos crediticios.
- Datos de actividad comercial o de servicios.
- Informes a entes de control
- Actas de comités
- Planes de auditoría
- Circulares
- Comprobantes financieros
- PQRSD que no contenga información de otros titulares sin previa autorización.

Tratamiento de datos personales de niños, niñas y adolescentes:

INDEPORTES ANTIOQUIA, acordado con el representante del menor, asegurará a través del consentimiento informado, el respeto de los derechos fundamentales de los niños, niñas y adolescentes, acatando las directrices y autorización de la persona responsable del menor, la cual debe velar porque los responsables del tratamiento cumplan con las leyes aquí mencionadas y reconocer que los niños, niñas y adolescentes, tienen derecho a ser escuchados y valorar su opinión, todo esto, de acuerdo a su madurez, autonomía y capacidad para entender el asunto.

INDEPORTES ANTIOQUIA garantizará la protección, respeto y adecuado tratamiento de los datos personales de los ciudadanos, niños, niñas y adolescentes, incluyendo disposiciones específicas para el tratamiento de registros fotográficos, contenido multimedia e historias clínicas en el marco de los servicios misionales, relacionados con la actividad física, apoyo psicosocial y medicina deportiva.

Derechos de los Titulares:

El titular que autoriza a INDEPORTES ANTIOQUIA el tratamiento de sus datos, tiene el derecho de:

- Conocer, actualizar y rectificar sus datos personales ante el encargado del tratamiento y puede validar si sus datos se encuentran inexactos, incompletos, fraccionados, o que el tratamiento esté prohibido o no haya sido autorizado por el titular.
- Solicitar prueba de la Autorización otorgada a INDEPORTES ANTIOUIA, salvo que la Ley indique que dicha Autorización no es necesaria.
- Presentar solicitudes ante INDEPORTES ANTIOQUIA o el Encargado del Tratamiento respecto del uso que le ha dado a sus Datos Personales, y a que se le entregue tal información.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la Ley.
- Revocar su Autorización y/o solicitar la supresión de sus Datos Personales de las bases de datos de INDEPORTES ANTIOQUIA, cuando la Superintendencia de Industria y Comercio haya determinado mediante acto administrativo definitivo que en el Tratamiento INDEPORTES ANTIOQUIA o el Encargado del Tratamiento ha incurrido en conductas contrarias a la Ley o cuando no hay una obligación legal o contractual de mantener el Dato Personal en la base de datos del responsable.
- Solicitar acceso y acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento de acuerdo con el artículo 21 del Decreto 1377 del 2013.
- Conocer las modificaciones a los términos de esta Política de manera previa y eficiente a la implementación de las nuevas modificaciones o, en su defecto, de la nueva política de tratamiento de la información.
- Tener fácil acceso a este documento y sus respectivas modificaciones.
- Acceder a los datos personales que se encuentran bajo el control de INDEPORTES ANTIOQUIA fácilmente de forma fácil y sencilla, para ejercer efectivamente los derechos que la Ley les otorga a los titulares.
- Conocer a la dependencia o persona facultada por INDEPORTES ANTIOQUIA frente a quien podrá presentar quejas, consultas, reclamos y cualquier otra solicitud sobre sus datos personales.
- Los titulares podrán ejercer sus derechos referente a datos personales a través de una solicitud formal por correo o a través del siguiente link: HTTPS://MERCURIO.INDEPORTESANTIOQUIA.GOV.CO/MERCURIO/INDICESERVLET?OPERACION=9&CODINDICE=00021&IDASUNTO=019&INDICADOR=1&LOGUEOPQR=S adjuntando carta de solicitud firmada y copia de cédula de ciudadanía. Si la solicitud es para un menor de edad, el acudientes o representante legal del menor, debe anexar además de los anteriores documentos, la copia de la identificación del menor.

Directrices de Interacción con el portal Web

INDEPORTES ANTIOQUIA, para tener interacción y un acercamiento con la ciudadanía en general y su participación activa, tiene a disposición el sitio web https://indeportesantioquia.gov.co el cual está sujeto

a términos condiciones de uso y confidencialidad en contenidos propios y contenidos externos protegidos por derechos de autor, en las que todos los ciudadanos al interactuar con el sitio deben aceptar los siguientes términos y condiciones. **En caso de no estar de acuerdo, abstenerse a usar este sitio web.**

Términos y Condiciones de uso:

1. El contenido de este sitio puede descargarse, usarse o modificarse únicamente con autorización directa de INDEPORTES ANTIOQUIA.
2. En caso de descargar información no autorizada desde el sitio web https://indeportesantioquia.gov.co, INDEPORTES ANTIOQUIA podrá tomar acciones las acciones legales y/o judiciales correspondientes.
3. INDEPORTES ANTIOQUIA, no concede ninguna licencia o autorización de uso de ninguna clase sobre sus derechos de propiedad intelectual, secretos empresariales o sobre cualquier otra propiedad o derecho relacionado con la página web y sus contenidos.
4. Si el usuario requiere realizar cualquier interacción en el sitio web en donde requiera ingresar sus datos personales, estos serán tratados de acuerdo con las **directrices de privacidad para el tratamiento de datos personales** mencionadas en este documento.
5. INDEPORTES ANTIOQUIA, se compromete a proteger la información de acuerdo con **el alcance** de este documento a nivel de confidencialidad, disponibilidad e integridad.
6. **Uso de las cookies**: INDEPORTES ANTIOQUIA, en su sitio web https://indeportesantioquia.gov.co utiliza cookies de sesión específicamente para entregar un mejor servicio al visitante y mejorar la experiencia del usuario al navegar por el portal.

Aceptación de términos y condiciones de uso del sitio web https://indeportesantioquia.gov.co

INDEPORTES ANTIOQUIA, da por entendido y aceptado los términos y condiciones de uso en el momento en que el usuario lea esta política y se constate el uso y utilización del sitio web https://indeportesantioquia.gov.co o una interacción en este mayor a 3 segundos, lo cual constituye un acuerdo legal entre la persona que ingresa al portal https://indeportesantioquia.gov.co.

ROLES Y RESPONSABILIDADES: Las responsabilidades se establecen teniendo en cuenta la estructura del Comité de la Gestión de la Información, y lo siguiente:

El Comité de Gestión y Desempeño: Establece y supervisa la alineación de los procedimientos, política general y manual de políticas seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales, con el sistema de gestión de Calidad y reporta el avance a la dirección, proponiendo nuevas estrategias para el tratamiento adecuado del riesgo de los activos de información y la protección de datos personales, procurando los recursos necesarios para el cumplimento de la implementación y a su vez, debe promover la mejora continua del sistema.

El representante de la estrategia Gobierno Digital (Gerente): Establece el enfoque para la política de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales, teniendo en cuenta la alineación de ésta con los objetivos y planes estratégicos de INDEPORTES ANTIOQUIA y el sistema de gestión de calidad, garantizando la puesta en marcha del sistema de gestión de la seguridad de la información.

El Líder de Gobierno Digital (Jefe de Sistemas): Coordina las actividades que tienen que ver con la gestión de la política de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad, el avance del manual y su articulación con el sistema de gestión de calidad, realizando un monitoreo al tratamiento de los riesgos de los activos de información y las estrategias de control relacionadas con las diferentes dependencias.

Líder área Jurídica: Se responsabilizará del aseguramiento y gestión de la protección y tratamiento de los datos personales.

Los usuarios, funcionarios, y contratistas: Se responsabilizan de cumplir con lo reglamentado en este documento, y lo plasmado en el manual de política de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales, articulándose con el comité de gestión y desempeño y jefes de procesos, para ayudar a que los activos de información y datos personales que estén en custodia y protección de un usuario, funcionario y/o contratista específico, estén cada vez más protegidos contra incidentes de seguridad.

Oficina Asesora de Comunicaciones: Se responsabilizan de gestionar y administrar la difusión de la información en materia de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales.

Oficina de Talento Humano: Se responsabilizan de gestionar y administrar las capacitaciones y sensibilizaciones programadas por la oficina de sistemas e informática relacionada con la seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales.

Oficina de Sistemas e Informática: Se responsabiliza de sensibilizar y capacitar a funcionarios, contratistas y partes interesadas en seguridad de la información, seguridad digital, ciberseguridad y la protección de datos personales

Oficina Asesora de Control Interno: Se responsabilizará validar el cumplimiento regulatorio e Incluir lo pertinente en materia de seguridad de la información, dentro de los planes de auditoría institucionales.

CONTROL DE LA INFORMACIÓN	RESPONSABLE
Elaborar	Funcionario y/o Contratista de la oficina de sistemas e Informática y de la oficina asesora jurídica.
Revisar	Jefe de oficina de sistemas e Informática y Jefe de Oficina Asesora Jurídica.
Aprobar	Gerente
Divulgar	Oficina Asesora de Comunicaciones.
Gestionar las capacitaciones	Oficina de Talento Humano
Sensibilizar	Oficina de Sistemas e informática y Oficina Asesora Jurídica
Anular	Comité de gestión y desempeño.
Validar cumplimiento	Oficina de Control Interno

RESPONSABLE	ACTIVIDADES/FUNCIONES
GERENTE Y COMITÉ DE GESTIÓN Y DESEMPEÑO	• Mantener la confidencialidad, integridad y disponibilidad de los activos de información y datos personales para la continuidad operativa y la buena prestación de los servicios de INDEPORTES ANTIOQUIA. • Realizar el tratamiento de los datos personales o realizar el encargo para lo propio.

	• Liderar y apoyar continuamente el modelo de la seguridad y privacidad de la información (aprobación de documentos, ejecución de las funciones asignadas en este sentido). • Garantizar que los recursos humanos, financieros e infraestructura se encuentren disponibles y se empleen de manera adecuada. • Hacer seguimiento y evaluar el modelo de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales, incluyendo temas alusivos en comités de gerencia en caso de que amerite.
JEFES DE OFICINA ASESORA Y JEFES DE OFICINA	• Implementar conjuntamente con el equipo de trabajo, estándares, guías, procedimientos o metodologías, con el fin de involucrarlos en las actividades de gestión de activos, y riesgos de seguridad de la información y protección de datos personales. • Aplicar controles para la continuidad de la seguridad, en cuanto a confidencialidad, integridad y disponibilidad de los activos de información y datos personales.
JEFE DE SISTEMAS	• Realizar de informes concretos a la alta gerencia sobre la implementación del modelo de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales. • Asesorar a las diferentes dependencias en la implementación del modelo de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales. • Desarrollar, mantener y comunicar las políticas, estándares, guías o metodologías de seguridad de la Información y protección de datos personales. • Desarrollar/administrar el análisis de riesgo de la seguridad de la información y protección a la privacidad de los datos personales. • Promover la cultura de seguridad de información y la protección de datos personales. • Proporcionar asistencia y asesoría a las áreas en el desarrollo de estándares y procedimientos, ciberseguridad, incidentes y evaluación de recursos tecnológicos para el cumplimiento de controles de la seguridad de información y protección de datos personales. • Informar a las partes interesadas en caso cualquier incidente de seguridad, referente a los riesgos que materializaron referentes a la seguridad de tecnología de la información, recursos de sistemas de información o tratamiento de datos personales. • Proporcionar apoyo para las nuevas iniciativas de seguridad de la información y protección de datos personales de la Institución. • Participar en la definición e implementación de los controles derivados de la política de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de los datos personales y de los planes de tratamiento de riesgos.

	• Adquirir las soluciones de seguridad informática necesarias para la entidad. • Proporcionar los reportes de análisis de seguridad de la información, a través de soporte técnico. • Asistir a los propietarios y usuarios de información, en asuntos de seguridad de plataformas específicas. • Nivelar los requerimientos de seguridad con las nuevas capacidades tecnológicas. • Por medio de la mesa de servicio TIC, monitorear grupos de usuarios, relacionado con medidas de seguridad específicas (listas de seguridad, páginas de seguridad, administración de contenidos, reportes de antivirus, aplicaciones, etc.) para generar reportes de vulnerabilidades. • Apoyar en la definición de indicadores y métricas para la medición de la eficiencia, eficacia y la efectividad de la implementación del modelo de seguridad y privacidad de la información. • Dirigir y coordinar la integración de los diferentes sistemas de gestión, con la seguridad de la información. • Articular y estandarizar, los procedimientos, metodologías y demás documentación requerida para el adecuado funcionamiento e integración de seguridad de la información en la entidad.
JEFE OFICINA DE TALENTO HUMANO	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. • Proporcionar el soporte logístico y metodológico para realizar las actividades de capacitación y concienciación en seguridad de información y protección de datos personal. • Actuar como enlace/articulador con sistemas de información, para el establecimiento de controles de acceso a los sistemas de información, con base al estado de vinculación y desvinculación de los funcionarios.
SUBGERENTE ADMINISTRATIVO Y FINANCIERO (INSTALACIONES LOCATIVAS)	• Evaluar las políticas y procedimientos de seguridad física, en temas relacionados con administración de instalaciones, control de acceso, control de vigilancia, controles ambientales, diseño y distribución de instalaciones. • Establecer y administrar los sistemas de control de acceso, para garantizar que las personas que se encuentren dentro de las instalaciones han sido debidamente autorizadas. • Revisar los logs generados por los sistemas de control de acceso. • Asegurar que cuando un funcionario se retire de la entidad, se recuperen todos los elementos que se encuentren en su posesión y

	que pertenezcan a la entidad (esto incluye activos físicos, tanto como digitales tales como archivos, contraseñas de acceso a plataformas etc. • Establecer y supervisar la vigilancia del edificio, adicionalmente constatar que los requerimientos de entrenamiento y conocimiento de los vigilantes sean cumplidos continuamente. • Realizar chequeos periódicos para determinar si las instalaciones actuales o propuestas de la entidad cumplen adecuadamente con normas de seguridad que permitan minimizar violaciones como robo, vandalismo, fuego, inundación, terremotos, terrorismo y en general cualquier violación que ponga en peligro la información de la entidad.
JEFE OFICINA DE CONTROL INTERNO	• Efectuar chequeos de cumplimiento donde se determine, el cumplimiento por parte de los funcionarios los diferentes procedimientos acerca del tratamiento de datos personales, las políticas de seguridad de activos de información y sus controles asociados. • Documentar y hacer seguimiento a los reportes que se hagan por los medios que tenga habilitados la entidad sobre problemas éticos, legales, violaciones a las políticas, comportamiento criminal, etc. • Evaluar periódicamente la efectividad de los controles de seguridad de información y procedimientos relacionados con el tratamiento de datos personales.
FUNCIONARIOS Y CONTRATISTAS	• Cumplir con todo lo definido en la política de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad. • Reportar cualquier actividad o comportamiento que pueda atentar contra la confidencialidad, integridad y disponibilidad de la información de la entidad. • Usar de manera responsable los recursos, activos físicos o digitales que tengan a su disposición por parte de la entidad • Participar en las actividades de sensibilización en seguridad de la información y tratamiento de datos personales, para garantizar que todo el personal está actualizado sobre estas temáticas.
ÁREA JURÍDICA	• Designar al oficial de tratamiento de datos personales que garantice el cumplimiento regulatorio relacionado este. • Establecer roles y responsabilidades propias del oficial de datos personales entre las cuales está: definir las cláusulas de confidencialidad, integridad y disponibilidad de la información que deban ser aplicadas a los contratos con terceros (sean personas naturales o jurídicas). Gestionar lo relacionado con la clasificación de la información y derecho del acceso a la misma (decreto 1712 de

	2014), gestionar todo lo relacionado con el cumplimento de la ley 1581 de 2012 y normatividad asociada. • Monitorear, evaluar y asesorar a las demás áreas sobre nueva legislación y nuevas regulaciones para definir lineamientos a considerar en cuanto a la seguridad de información, tratamiento de datos personales y aspectos relacionados con la privacidad. • Realizar de informes concretos a la alta gerencia sobre la protección de los datos personales. • Asesorar a las diferentes dependencias en la protección de os datos personales. • Desarrollar, mantener y comunicar las políticas, estándares, guías o metodologías de protección de datos personales. • Desarrollar/administrar el análisis de riesgo de la protección de los datos personales. Promover la cultura de la protección de datos personales.
POR DEFINIR	• Validar implicaciones disciplinarias a funcionarios referentes a la seguridad de información. • Dar inicio a los procesos disciplinarios que se deriven del no cumplimiento con las políticas internas, estándares u otros requerimientos de seguridad de información.

FUNDAMENTOS DE LA POLÍTICA: Los fundamentos de la política de seguridad de la información, seguridad digital, ciberseguridad y protección de la privacidad de INDEPORTES ANTIOQUIA, se establecen teniendo en cuenta las directrices estipuladas por el Comité de Gestión y Desempeño y su representante.

NORMATIVIDAD APLICABLE:

NORMATIVA	DESCRIPCIÓN DE LA NORMATIVA
Ley 594 de 2000	"Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
Ley 1098 de 2006	Código de Infancia y Adolescencia, principios de prevalencia de los derechos de los niños, niñas y adolescentes.
Ley 1150 de 2007	"Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos".
Ley 1341 de 2009	"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".
Ley 1581 de 2012	"Por medio de la cual se dictan disposiciones generales para la protección de datos personales".
Ley 1712 de 2014	"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
Decreto 2609 de 2012	"Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 1377 de 2013	"Por la cual se reglamenta parcialmente la Ley 1581 de 2012".
Decreto 886 de 2014	"Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".
Decreto 1074 de 2015	por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo y se reglamenta el Registro Nacional de Bases de Datos.
Decreto 1078 de 2015	Por medio de la cual se establece el Decreto Único Reglamentario del sector de tecnologías de la información y las comunicaciones.
Decreto 1083 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública".
Decreto 1085 de 2015	En lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

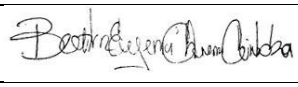
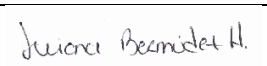
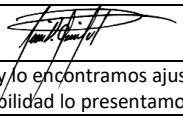
Decreto 0103 de 2015	“Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones”.
Decreto 0415 de 2016	“Por el cual se adiciona el Decreto único reglamentario del sector de la función pública”.
CONPES 3701 de 2011	"Lineamientos de política para la Ciberseguridad y Ciberdefensa".
CONPES 3995 de 2020	“Política Nacional de Confianza y de Seguridad Digital”.
Decreto 338 de 2022	Establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, y un Marco de Ciberseguridad Nacional, fortalece la protección de infraestructuras críticas y sistemas de información en el país y Proporciona orientación sobre las medidas de seguridad de la información en la computación en nube.
Decreto 767 de 2022.	Por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 2294 de 2023	“Por la cual se expide el Plan Nacional de Desarrollo 2022-2026- Colombia potencia mundial de la vida”.
Resolución Institucional RS2018000293 de 2018	“Por la cual se establece el comité de gestión y desempeño de INDEPORTES ANTIOQUIA”
RS 2023001322	Por medio de la cual se actualizan las políticas, estándares de seguridad y uso de los recursos informáticos en INDEPORTES ANTIOQUIA.
RS2020000514	Por medio de la cual se actualizan las políticas, estándares de seguridad y uso de los recursos informáticos en INDEPORTES ANTIOQUIA.
RS2021000024	Por medio de la cual se adopta la política de tratamiento de datos personales en el Instituto departamental de deportes de Antioquia INDEPORTES ANTIOQUIA (derogada por esta política)
Resolución Institucional RS2024000757	“Por la cual se realiza una modificación en relación con los integrantes y las funciones del Comité de Gestión y Desempeño institucional y se adopta el Sistema de Gestión con el nuevo Modelo de Planeación y Gestión MIPG”.

Estándares Internacionales

- ISO 27001: Establece los requisitos para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO 27002: Establece los controles para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO 9001: Establece los requisitos para implementar un Sistema de Gestión de la Calidad (SGC).
- NIST: Instituto Nacional de Estándares de Tecnología.

GESTION DE RIESGOS: La gestión y tratamiento de los riesgos de la Seguridad de la Información, la Seguridad Digital, la Ciberseguridad y la Protección de la Privacidad de los Datos Personales de INDEPORTES ANTIOQUIA que preside esta política, se basan en la metodología de riesgos que actualmente rige la entidad, en el marco de referencia de gestión de riesgos del sistema de Gestión de Calidad de la Institución y de la normativa de Gobierno Digital del Ministerio de las TIC.

LUIS GIOVANY ARIAS TOBON
Gerente

	NOMBRE	FIRMA	FECHA
Proyectó	Beatriz Eugenia Chaverra Córdoba Contratista TI		14/05/2025
Proyecto	María Teresa Muñoz PU – Oficina Asesora Jurídica		14/05/2025
Reviso	Juliana Bermúdez Henao Jefe Oficina de sistemas		14/05/2025
Revisó	León David Quintero Restrepo Jefe Oficina Asesora Jurídica		14/05/2025
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			