POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. NORMATIVIDAD

La presente política se fundamenta en el Plan de Seguridad y Privacidad de la Información (PSPI) y en la normatividad nacional aplicable a las entidades públicas, en especial aquellas que regulan la protección de datos personales y la seguridad digital. Entre ellas:

- Constitución Política de Colombia (arts. 15, 209 y 269).
- Ley 1581 de 2012 – Protección de datos personales.
- Decreto 2609 de 2012 – Gestión documental en entidades del Estado.
- Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014 – Registro Nacional de Bases de Datos.
- Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Decreto 103 de 2015 – Reglamentación parcial de la Ley 1712 de 2014.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC.
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- Ley 1915 de 2018 – Reformas en materia de derecho de autor.
- Decreto 612 de 2018 – Directrices para la integración de planes institucionales.
- Decreto 2106 de 2019 – Estrategia de seguridad digital en trámites y procesos estatales.
- Ley 1952 de 2019 – Código General Disciplinario.

2. OBJETIVO

Definir los lineamientos establecidos por el Instituto Municipal de Deporte y Recreación de Yumbo – IMDERTY en materia de seguridad y privacidad de la información, de conformidad con el PSPI, las políticas de Seguridad Digital y Gobierno Digital, los requisitos legales vigentes y las necesidades de la comunidad deportiva, recreativa y administrativa.

El propósito es consolidar el PSPI, que asegure la confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio de la información generada y administrada por el IMDERTY en el desarrollo de sus funciones misionales, garantizando así la confianza ciudadana y la eficiencia institucional.

3. DEFINICIONES Y GLOSARIO

- Acceso a la Información Pública: Derecho que tienen todas las personas a conocer la información generada, administrada o en poder del IMDERTY, conforme a la Ley 1712 de 2014 (Ley de Transparencia).
- Activo: Cualquier bien, recurso, servicio o elemento de valor para el IMDERTY, tangible o intangible, que contribuye al cumplimiento de los objetivos institucionales.
- Activos de Información: Conjunto de datos, documentos, registros, aplicaciones, infraestructura tecnológica o conocimiento que posee valor para la gestión institucional y que debe ser protegido.

- Amenaza: Potencial causa de un incidente que puede provocar daños a un activo de información y, por ende, afectar la operación del IMDERTY.
- Autenticidad: Propiedad que permite identificar con certeza el origen y autoría de la información, garantizando la confianza en su procedencia.
- Clasificación de la Información: Proceso mediante el cual se determina el nivel de sensibilidad y protección que debe aplicarse a los activos de información del IMDERTY.
- Confidencialidad: Propiedad que asegura que la información solo sea accesible a personas, procesos o sistemas autorizados.
- Confidencialidad, Integridad y Disponibilidad (CID): Principios básicos de la seguridad de la información que buscan proteger la información frente a accesos no autorizados, modificaciones indebidas y pérdidas de disponibilidad.
- Controles: Medidas administrativas, técnicas, físicas o legales implementadas para reducir riesgos que puedan afectar la seguridad de la información.
- Control: Acción o disposición específica que busca prevenir, detectar o mitigar amenazas que comprometan la información del IMDERTY.
- Continuidad: Capacidad del IMDERTY para mantener la operación de sus procesos misionales y de apoyo, incluso ante incidentes o contingencias, en línea con los planes de continuidad institucional.
- Dato Personal: Información que identifica o permite identificar a una persona natural, según lo definido en la Ley 1581 de 2012.
- Dato Sensible: Información personal que, de acuerdo con la Ley 1581 de 2012, afecta la intimidad de la persona o cuyo uso indebido puede generar discriminación (salud, orientación política, origen étnico, creencias religiosas, entre otros).
- Disponibilidad: Cualidad que garantiza que la información y los sistemas estén accesibles y utilizables en el momento en que se requieran para la gestión institucional.
- Gestión de Seguridad de la Información: Conjunto de actividades coordinadas para dirigir y controlar la seguridad de la información dentro del IMDERTY.
- Incidente de Seguridad de la Información: Evento adverso que compromete o puede comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información del IMDERTY.
- Integridad: Propiedad que asegura que la información permanece completa, exacta y sin alteraciones no autorizadas.
- Plan de Seguridad y Privacidad de la Información (PSPI): Directriz oficial del Ministerio TIC que orienta a las entidades públicas en la gestión de la seguridad y privacidad de la información.
- No Repudio: Principio que asegura que una persona no pueda negar la autoría o recepción de una comunicación, transacción o actuación previamente realizada.
- Política de Seguridad de la Información: Declaración formal del IMDERTY que establece directrices, compromisos y lineamientos para garantizar la protección de la información.
- Privacidad: Derecho fundamental que busca proteger los datos personales en concordancia con la Ley 1581 de 2012 y sus decretos reglamentarios.
- Recursos: Bienes humanos, tecnológicos, financieros y logísticos que el IMDERTY utiliza para gestionar y proteger sus activos de información.
- Responsabilidad: Obligación que tienen los servidores públicos, contratistas y terceros de

cumplir con las disposiciones establecidas en la Política de Seguridad y Privacidad de la Información del IMDERTY.

- Riesgo: Posibilidad de que una amenaza se materialice y afecte negativamente la confidencialidad, integridad, disponibilidad o privacidad de la información.
- Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de políticas, procedimientos, procesos y controles implementados en el Instituto
- Municipal del Deporte y la Recreación de Yumbo IMDERTY para gestionar la seguridad de la información, en concordancia con el PSPI.
- Transparencia: Principio que garantiza la visibilidad, acceso y publicidad de la información en poder del IMDERTY, salvo aquella clasificada como reservada o confidencial según la ley.
- Usuarios: Personas internas o externas que acceden a la información, sistemas y recursos del IMDERTY bajo los permisos establecidos.
- Vulnerabilidad: Debilidad en un activo de información, proceso, sistema o control que puede ser explotada por una amenaza y afectar la seguridad de la información.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

En el IMDERTY cuidamos la información como un recurso valioso para la institución y la comunidad. Nuestra política general es protegerla para que siempre esté segura, completa y disponible cuando se necesite, cumpliendo con las leyes sobre transparencia, acceso a la información pública y protección de datos personales. Nos comprometemos a manejar los riesgos que puedan afectar los datos, los sistemas o los servicios de información, garantizando un acceso responsable que diferencie entre lo que es público, reservado o confidencial. Todos los funcionarios, contratistas y terceros son responsables del cuidado de la información que usan, asegurando la continuidad de los sistemas y procesos incluso en caso de incidentes o emergencias. También fomentamos la cultura de seguridad enseñando buenas prácticas y el manejo adecuado de la información, y trabajamos en mejorar constantemente las medidas de seguridad y privacidad, adaptándonos a los cambios tecnológicos y a las necesidades del IMDERTY.

5. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Fortalecer la cultura de seguridad de la información en la infraestructura tecnológica a cargo de funcionarios, terceros, aprendices, practicantes y ciudadanos que pertenezcan o visiten el IMDERTY por medio de un plan de capacitación y concientización el cual debe ejecutarse permanentemente y que alcance a todos los funcionarios públicos, contratistas y los interesados en la gestión de la seguridad de la información en el IMDERTY.
- Establecer e implementar los controles que requieren planes, procedimientos e instructivos en materia de seguridad de la información por medio de planes de seguridad y privacidad que anualmente se ejecuten con actividades técnicas requeridas.
- Minimizar el riesgo de todos los procesos del IMDERTY donde anualmente se identifiquen, analicen, valoren y mitiguen los riesgos asociados al objeto social del IMDERTY, por medio de un plan de gestión y tratamiento de riesgos.
- Mejorar continuamente el PSPI.

- Implementar los controles tecnológicos necesarios para la protección de los activos del IMDERTY y para la reducción de los riesgos.

6. COMPROMISO DE LA GERENCIA

El IMDERTY en cabeza del Gerente se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del proceso Gestión de Tecnología, Información y Comunicación. Así mismo, se compromete a revisar el avance de la implementación de manera periódica y garantizar los recursos suficientes y necesarios (tecnológicos y talento humano calificado) para implementar y mantener el sistema. De igual forma, incluirá dentro de las decisiones estratégicas la seguridad de la información.

7. ALCANCE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La implementación del PSPI, conforme a los requisitos normativos, comprende a todos los procesos del IMDERTY

Esta política debe ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo hardware y/o software de propiedad o en uso por parte del IMDERTY, así mismo por todos los usuarios que hacen uso de la infraestructura de comunicaciones de las redes internas y de los servicios de internet, como las redes wifi disponibles para funcionarios del IMDERTY, ciudadanos y visitantes en las redes públicas.

Esta política tiene como propósito reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad de las funciones misionales del IMDERTY.

8. APLICABILIDAD

La presente política, sus objetivos, además de procesos o documentos derivados o complementarios, aplican a todo el IMDERTY, a sus servidores públicos, contratistas y terceros vinculados, así como a aquellas personas que, en razón del cumplimiento de sus funciones o de las del IMDERTY , compartan, utilicen, recolecten, procesen, intercambien o consulten su información, y a las demás entidades relacionadas que accedan, ya sea interna o externamente, a cualquier activo de información, independientemente de su ubicación.

De igual manera, esta política aplica a toda la información creada, procesada o utilizada por el IMDERTY, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

El incumplimiento a la PSPI o de sus lineamientos derivados traerá consigo las consecuencias legales correspondientes según la normativa aplicable al IMDERTY.

9. SANCIONES

Cualquier violación a las políticas de seguridad de la información del IMDERTY será sancionada de acuerdo con el Reglamento Interno de Trabajo, las normas y leyes colombianas aplicables, incluyendo lo establecido en materia de delitos informáticos.

Las sanciones dependerán de la gravedad de la falta, sus consecuencias y la intencionalidad con que se haya cometido.

10. PROCESO JURIDICO

Dentro de la estrategia de seguridad de la información, el IMDERTY establece un procedimiento disciplinario formal para los funcionarios, contratistas o terceros.

El proceso jurídico busca no solo aplicar las medidas correctivas necesarias, sino también servir como herramienta de prevención para evitar nuevas violaciones a la política o al programa de seguridad y privacidad de la información.

Se consideran violaciones a la seguridad y privacidad de la información en el IMDERTY entre otras:

- Omitir la actualización, entrega o devolución de los activos de información asignados para el desarrollo de sus funciones o procesos.
- Ingresar o acceder a información confidencial de otros procesos sin la autorización previa del responsable de la información.
- No reportar oportunamente eventos y/o incidentes de seguridad de la información, o situaciones sospechosas que puedan vulnerar la política de seguridad y privacidad de la información.
- No seguir los lineamientos de clasificación de información, generando registros o clasificaciones inadecuadas.
- Exponer información confidencial o de uso interno en formato impreso sin las medidas mínimas de seguridad, al ausentarse del puesto de trabajo o al finalizar la jornada laboral.
- Dejar gavetas, escritorios o archivadores abiertos o con llaves puestas cuando en ellos se guarde información confidencial o de uso interno.
- No apagar los equipos de cómputo al terminar la jornada laboral.
- Sustraer o almacenar información del IMDERTY en dispositivos externos sin autorización previa.
- Solicitar cambio de contraseña de un usuario diferente al propio sin la debida autorización del titular o de su superior inmediato.
- Utilizar la red de datos del IMDERTY para obtener, mantener o difundir material ofensivo, no permitido, cadenas de correos o correos masivos no autorizados.
- Descargar o utilizar software ajeno a las funciones del cargo, que pueda afectar la plataforma tecnológica del IMDERTY.
- Compartir información institucional a través de correos electrónicos personales distintos a los asignados por el IMDERTY.
- Compartir información confidencial o de uso interno, en formato físico o digital, sin aplicar los protocolos definidos para su divulgación.

- Utilizar equipos tecnológicos desatendidos o que, a través de sistemas inalámbricos, transmitan, reciban o almacenen datos sin las debidas medidas de seguridad.

- Permitir el acceso de funcionarios, contratistas o terceros a la red corporativa sin autorización expresa del responsable del proceso de gestión TIC del IMDERTY.

- Dar un uso inadecuado o no garantizar el cuidado de equipos, dispositivos portátiles o móviles entregados para el desarrollo de las actividades en el IMDERTY.

- No cumplir con las actividades designadas para la protección de los activos de información del IMDERTY.

- Eliminar, destruir, modificar o desechar de manera incorrecta documentación institucional.

- Descuidar documentación con información confidencial o de uso interno, sin aplicar medidas apropiadas de protección.

- Registrar información confidencial en pos-it, apuntes, agendas o libretas, dejándola expuesta a la vista de personal no autorizado.

- Archivar información confidencial o de uso interno sin claves de seguridad, cifrado u otras medidas de protección.

- Usar los recursos tecnológicos del IMDERTY para fines o beneficios personales.

- Acceder sin autorización a sistemas informáticos institucionales o permanecer en ellos en contra de la voluntad del IMDERTY

- Impedir u obstaculizar, sin autorización, el funcionamiento o acceso normal a los sistemas, datos informáticos o redes del IMDERTY.

- Destruir, dañar, alterar o suprimir datos informáticos o sistemas de tratamiento de información del IMDERTY.

- Propagar o distribuir software malicioso u otros programas de computación con efectos dañinos en la plataforma tecnológica.

- Administrar de manera incorrecta los datos personales contenidos en las bases de datos del IMDERTY.

- Suplantar la identidad de un usuario en los sistemas de autenticación y autorización del IMDERTY.

- Compartir con otros usuarios las contraseñas de acceso a la red de datos, recursos tecnológicos o sistemas de información del IMDERTY.

- Permitir el acceso u otorgar privilegios a las redes de datos del IMDERTY a personas no autorizadas.

- Realizar actividades fraudulentas o ilegales, o intentar el acceso no autorizado a cualquier

computador, sistema o equipo del IMDERTY o de terceros.

- Ejecutar acciones tendientes a evitar o incumplir los controles de seguridad establecidos por el IMDERTY.
- Retirar de las instalaciones estaciones de trabajo, computadores portátiles u otros equipos que contengan información institucional sin autorización expresa.
- Sustraer, abandonar o trasladar documentos con información corporativa clasificada como confidencial o de uso interno sin autorización.
- No realizar el borrado seguro de información contenida en equipos o dispositivos de almacenamiento del IMDERTY al momento de su traslado, reasignación o disposición final.
- Ejecutar acciones que atenten contra la reputación, imagen o buen nombre del IMDERTY.
- Realizar cambios no autorizados en la plataforma tecnológica del IMDERTY.
- Acceder, almacenar o distribuir material prohibido por la ley, incluyendo pornografía infantil.
- Instalar programas o software no autorizados por el área de TIC del IMDERTY.
- Copiar sin autorización programas del IMDERTY, o infringir derechos de autor y acuerdos de licenciamiento relacionados con software.

11. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL PSPI

El IMDERTY, indica que realizará revisiones periódicas al PSPI. Dichas revisiones estarán enfocadas en los siguientes aspectos

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información, los cuales pueden ser basados en la gestión del riesgo, teniendo en cuenta la cantidad de actividades propuestas versus las ejecutadas y las monitoreadas y validadas, basadas en los resultados
- Obtenidos de informes de seguimiento y en cantidad de eventos de seguridad basados en tiempo, sean meses, semanas, o días.
- Revisión de avance en la implementación del Plan de Seguridad y Privacidad de la Información del IMDERTY.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

12. REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Gerencia del IMDERTY. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.

2. Si se dan cambios estructurales en el IMDERTY (restructuración de procesos).

3. Incidentes de seguridad de la información que requieran que la política requiere cambios, basados en normativas para implementar o requerimientos legales que deban ser tenidos en cuenta por el IMDERTY.

ARTHUR MILTON PALACIO VILLALOBOS
GERENTE