RESOLUCIÓN N° 176 DE 2025
(18 DE SEPTIEMBRE DE 2025)

"POR MEDIO DE LA CUAL SE IMPLEMENTA LA POLÍTICA DE SEGURIDAD DIGITAL DEL INSTITUTO MUNICIPAL DE DEPORTES Y RECREACIÓN DE CAJICÁ – INSDEPORTES CAJICÁ Y SE ESTABLECEN OTRAS DISPOSICIONES"

el director del instituto municipal de deportes y recreación de Cajicá – Insdeportes Cajicá, en ejercicio de sus atribuciones legales y estatutarias, en especial las conferidas por el Acuerdo Municipal No. 024 de 1996, modificado por el Acuerdo Municipal No. 011 de 1999, la Ley 489 de 1998, la Ley 1712 de 2014, el Decreto 1499 de 2017, el Decreto 767 de 2022, y

I. CONSIDERANDO.

Que la Constitución Política de Colombia consagra a Colombia como un Estado Social de Derecho, fundado en el respeto de la dignidad humana, la prevalencia del interés general y la garantía de los derechos fundamentales, y establece como fines esenciales del Estado, entre otros, servir a la comunidad, garantizar la efectividad de los derechos y asegurar la prestación eficiente de los servicios públicos (artículos 1 y 2).

Que el artículo 209 de la Constitución Política dispone que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de legalidad, igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, así como en el deber de las autoridades administrativas de coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado.

Que el artículo 15 de la Constitución Política reconoce el derecho fundamental a la intimidad personal y familiar, al buen nombre y a la protección de los datos personales, imponiendo al Estado el deber de garantizar su respeto y protección, lo cual resulta plenamente aplicable en el entorno digital y en el tratamiento de la información que administran las entidades públicas.

Que la Ley 1581 de 2012 y la Ley 1712 de 2014 establecen el marco legal para la protección de datos personales y el acceso a la información pública, imponiendo a las entidades públicas el deber de adoptar medidas técnicas, administrativas y organizacionales que garanticen el tratamiento seguro de la información y la protección de los derechos de los titulares.

Que la Ley 489 de 1998, en su artículo 4°, dispone que la función administrativa busca la satisfacción de las necesidades generales de los habitantes, consultando en todo momento el interés general, y que las entidades descentralizadas se sujetan a la Constitución, la ley y a sus estatutos internos, desarrollando su gestión conforme a los principios de democracia participativa, control social y responsabilidad administrativa.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

Que el Modelo Integrado de Planeación y Gestión – MIPG, adoptado mediante el Decreto 1499 de 2017 y compilado y actualizado por el Decreto 767 de 2022, establece la Seguridad Digital como una política de gestión y desempeño, orientada a preservar la confidencialidad, integridad y disponibilidad de la información, fortalecer la confianza digital, gestionar los riesgos asociados al uso de tecnologías y asegurar la continuidad de los servicios públicos.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, en desarrollo de la Política de Seguridad Digital, ha definido lineamientos y buenas prácticas para que las entidades públicas adopten esquemas institucionales de gestión del riesgo digital, protección de activos de información, prevención de incidentes de seguridad y fortalecimiento de la resiliencia organizacional, en coherencia con la Estrategia Nacional de Seguridad Digital.

Que mediante el Acuerdo Municipal No. 024 de 1996, modificado por el Acuerdo Municipal No. 011 de 1999, se creó el Instituto Municipal de Deportes y Recreación de Cajicá – INSDEPORTES CAJICÁ como entidad descentralizada del orden municipal, con la competencia de formular políticas y ejecutar planes, programas y proyectos en materia de deporte, recreación, actividad física y aprovechamiento del tiempo libre.

Que INSDEPORTES CAJICÁ, en el desarrollo de sus funciones misionales, administrativas, financieras, contractuales y de atención a la ciudadanía, hace uso permanente de plataformas tecnológicas, sistemas de información, bases de datos y medios digitales, los cuales contienen información institucional y datos personales que deben ser protegidos frente a riesgos de pérdida, alteración, uso indebido o acceso no autorizado.

Que la adecuada gestión de la seguridad digital constituye un elemento esencial para garantizar la legalidad de las actuaciones administrativas, la protección de los derechos fundamentales, la continuidad del servicio público, la transparencia institucional y la confianza de la ciudadanía, servidores públicos, contratistas y demás partes interesadas.

Que, en armonía con el Plan de Desarrollo Municipal "Cajicá Ideal 2024–2027", el cual promueve la modernización administrativa, la eficiencia institucional y el fortalecimiento de la gestión pública, resulta necesario implementar formalmente la Política de Seguridad Digital en INSDEPORTES CAJICÁ, como instrumento de gestión que permita prevenir, mitigar y gestionar los riesgos digitales, y fortalecer el cumplimiento de los principios constitucionales y legales que rigen la función administrativa.

Que, en virtud de lo anterior, se hace procedente adoptar la Política de Seguridad Digital del Instituto Municipal de Deportes y Recreación de Cajicá – INSDEPORTES CAJICÁ, así como el Plan de Acción que la desarrolla, en el marco del Modelo Integrado de Planeación y Gestión – MIPG.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

II. RESUELVE.

ARTÍCULO PRIMERO. Implementación de la Política. Implementar la Política de Seguridad Digital del Instituto Municipal de Deportes y Recreación de Cajicá – INSDEPORTES CAJICÁ, como una política institucional transversal, en armonía con la Política de Seguridad Digital definida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, el Modelo Integrado de Planeación y Gestión – MIPG y la normativa vigente.

ARTÍCULO SEGUNDO. Ámbito de aplicación. La Política de Seguridad Digital será de obligatorio cumplimiento para todos los servidores públicos, contratistas, proveedores y terceros que, en razón de sus funciones o actividades, tengan acceso a los activos de información, sistemas, plataformas tecnológicas o recursos digitales del Instituto Municipal de Deportes y Recreación de Cajicá.

ARTÍCULO TERCERO. Responsables de la implementación. La Dirección del Instituto será la responsable de liderar la implementación de la Política de Seguridad Digital, con el apoyo de los procesos administrativos y misionales, conforme a sus competencias, en el marco del Modelo Integrado de Planeación y Gestión – MIPG.

ARTÍCULO CUARTO. Seguimiento. El seguimiento a la implementación de la Política de Seguridad Digital y de su Plan de Acción estará a cargo del Comité Institucional de Gestión y Desempeño, en el marco de la Dimensión de Evaluación de Resultados del MIPG, y deberá registrarse en los instrumentos institucionales de seguimiento, autoevaluación y reporte, garantizando la trazabilidad de las acciones y el cumplimiento de los objetivos de la Política.

ARTÍCULO QUINTO. Evaluación. La evaluación de la Política de Seguridad Digital estará a cargo del Proceso de Gestión Jurídica, con el acompañamiento y verificación del Proceso de Control Interno, en el marco de la Dimensión de Control Interno del Modelo Integrado de Planeación y Gestión – MIPG, conforme al esquema de líneas de defensa adoptado por la entidad.

La evaluación tendrá como propósito verificar la legalidad, coherencia normativa, alineación institucional y pertinencia jurídica de la Política y de su implementación, así como el cumplimiento de los principios de la función administrativa y de los lineamientos de seguridad digital vigentes.

Los resultados de la evaluación servirán como insumo para la mejora continua, la actualización de la Política y la adopción de acciones preventivas o correctivas, cuando a ello haya lugar.

ARTÍCULO SEXTO. Responsables. Publicidad. La presente resolución y la Política de Seguridad Digital deberán ser publicadas a través de los canales institucionales del Instituto Municipal de Deportes y Recreación de Cajicá – INSDEPORTES CAJICÁ, garantizando su acceso, conocimiento y consulta por parte de los servidores públicos, contratistas y demás partes interesadas.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

ARTÍCULO SÉPTIMO. Socialización. La Dirección del Instituto dispondrá la socialización interna y externa de la presente resolución y de la Política de Seguridad Digital, dirigida a los servidores públicos, contratistas, proveedores y terceros que tengan acceso a los activos de información y recursos digitales del Instituto, a fin de garantizar su conocimiento, apropiación y aplicación efectiva.

ARTÍCULO OCTAVO. Vigencia. La presente resolución rige a partir de la fecha de su expedición y publicación, y la Política de Seguridad Digital se mantendrá vigente mientras no sea modificada, actualizada o derogada mediante acto administrativo posterior, sin perjuicio de los ajustes que se realicen como resultado del seguimiento y evaluación en el marco del Modelo Integrado de Planeación y Gestión – MIPG.

ARTÍCULO NOVENO. Aplicación. La presente resolución será de aplicación exclusiva para los fines dispuestos en el presente acto administrativo, en lo relacionado con la implementación, cumplimiento y fortalecimiento de la Política de Seguridad Digital del Instituto Municipal de Deportes y Recreación de Cajicá – INSDEPORTES CAJICÁ.

PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE,

Expedida en Cajicá - Cundinamarca, a los dieciocho (18) días del mes de septiembre de dos mil veinticinco (2025).

DUVÁN ALEJANDRO LÓPEZ CALDERÓN
Director

Responsable	Nombre(s) y apellidos	Firma	Proceso
Proyectó	Roxan Elena González Tapia		Jefe - Gestión Jurídica
Revisó	Herson Yesid Arroyo Acevedo		Asesor - Gestión Jurídica
Revisó y aprobó	Duván Alejandro López Calderón		Director
Los firmantes, manifestamos expresamente que hemos estudiado y revisado el presente documento, y por encontrarlo ajustado a las disposiciones constitucionales, legales y reglamentarias vigentes, lo presentamos para su firma bajo nuestra responsabilidad.			

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

ANEXOS

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

ANEXO 1

POLÍTICA DE SEGURIDAD DIGITAL

INSTITUTO MUNICIPAL DE DEPORTES Y RECREACIÓN DE CAJICÁ – INSDEPORTES CAJICÁ

La presente Política de Seguridad Digital del Instituto Municipal de Deportes y Recreación de Cajicá – INSDEPORTES CAJICÁ se articula de manera transversal con los instrumentos de planeación estratégica, gestión institucional y control definidos en el orden nacional y territorial, garantizando coherencia normativa, eficiencia administrativa y generación de valor público.

En este sentido, la Política se armoniza con el Plan Estratégico de Tecnologías de la Información – PETI, en cuanto orienta el uso seguro, responsable y eficiente de las tecnologías que soportan los procesos misionales, estratégicos y de apoyo del Instituto, asegurando que la planeación tecnológica incorpore criterios de gestión del riesgo, continuidad operativa, protección de la información y sostenibilidad digital.

Así mismo, la Política se articula con la Política de Gobierno Digital, en tanto fortalece los habilitadores transversales de seguridad y privacidad de la información, gestión de datos, servicios digitales confiables y toma de decisiones basadas en información íntegra, disponible y protegida, contribuyendo al cumplimiento de los principios de eficiencia, transparencia, interoperabilidad y confianza digital en la relación Estado–ciudadanía.

De igual manera, la presente Política se encuentra alineada con el Modelo de Seguridad y Privacidad de la Información – MSPI, incorporando los principios de confidencialidad, integridad y disponibilidad, así como la gestión de riesgos, el tratamiento de incidentes de seguridad, la definición de responsabilidades y la mejora continua de los controles institucionales, en concordancia con la Dimensión de Control Interno del Modelo Integrado de Planeación y Gestión – MIPG.

La articulación entre la Política de Seguridad Digital, el PETI y la Política de Gobierno Digital garantiza que las decisiones tecnológicas del Instituto no se limiten a aspectos operativos, sino que respondan a un enfoque estratégico, preventivo y jurídico-administrativo, orientado a proteger los activos de información, asegurar la continuidad del servicio público y fortalecer la confianza de la ciudadanía, los funcionarios, contratistas y demás grupos de valor.

1. INTRODUCCIÓN

La Seguridad Digital constituye un componente esencial de la gestión institucional de INSDEPORTES CAJICÁ, en tanto permite proteger los activos de información, garantizar la continuidad del servicio público y fortalecer la confianza de la ciudadanía, los servidores públicos y los contratistas en el uso de las tecnologías de la información.

La presente Política establece los lineamientos generales para la protección de la información institucional, independientemente del medio, formato o plataforma utilizada, y

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

6. ARMONIZACIÓN INSTITUCIONAL

Esta Política se articula de manera transversal con el Plan Estratégico de Tecnologías de la Información – PETI, la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información – MSPI, en el marco del Modelo Integrado de Planeación y Gestión – MIPG, garantizando coherencia normativa, gestión del riesgo, control interno efectivo y mejora continua de la gestión institucional.

7. DEFINICIONES

Para efectos de la presente Política de Seguridad Digital, se adoptan las siguientes definiciones, las cuales orientan su interpretación, aplicación y cumplimiento:

Acción correctiva: Medida orientada a eliminar la causa de una amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

Acción preventiva: Medida orientada a prevenir la materialización de amenazas o riesgos que afecten la seguridad de la información.

Activo de información: Datos, documentos o información con valor para la Entidad, independientemente de su formato o medio.

Amenaza: Circunstancia o suceso con potencial de afectar un sistema de información.

Análisis de riesgo: Proceso para identificar, evaluar y priorizar riesgos de seguridad de la información.

Aplicaciones: Programas o software utilizados para la gestión y control de la información institucional.

Autenticación: Proceso de verificación de identidad para acceder a sistemas o información.

Backup (copia de respaldo): Procedimientos para garantizar la recuperación de la información.

Confidencialidad: Garantía de que la información solo sea accesible a personas autorizadas.

Control: Medida orientada a mantener los riesgos dentro de niveles aceptables.

Denegación de servicio: Ataque que limita o impide el acceso legítimo a un sistema.

Disponibilidad: Garantía de acceso oportuno a la información.

Dispositivo: Equipo tecnológico utilizado para acceder a sistemas institucionales.

Evento de seguridad: Suceso que evidencia una posible afectación a la seguridad de la información.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

se orienta a prevenir, detectar y responder de manera oportuna a los riesgos e incidentes de seguridad digital que puedan afectar el cumplimiento de los fines institucionales.

2. MARCO NORMATIVO

La presente Política de Seguridad Digital se fundamenta, entre otras, en las siguientes disposiciones constitucionales, legales y administrativas:

- Constitución Política de Colombia, artículos 1, 2, 15, 209 y 365.
- Ley 489 de 1998, sobre organización y funcionamiento de las entidades públicas.
- Ley 1581 de 2012, sobre protección de datos personales y sus normas reglamentarias.
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Decreto 1499 de 2017 y Decreto 767 de 2022, por los cuales se adopta y actualiza el Modelo Integrado de Planeación y Gestión – MIPG.
- Lineamientos y Política de Seguridad Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Plan de Desarrollo Municipal "Cajicá Ideal 2024–2027", en lo relacionado con modernización institucional, transformación digital y fortalecimiento de la gestión pública.

3. OBJETIVO GENERAL

Establecer los lineamientos institucionales para la gestión de la Seguridad Digital en INSDEPORTES CAJICÁ, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la prevención, detección y respuesta frente a riesgos e incidentes de seguridad digital.

4. OBJETIVOS ESPECÍFICOS

4.1. Identificar las herramientas tecnológicas institucionales utilizadas para la generación, procesamiento, almacenamiento y consulta de información.

4.2. Definir parámetros generales de uso seguro de las herramientas tecnológicas por parte de servidores públicos y contratistas.

4.3. Establecer medidas técnicas, administrativas y organizacionales para la protección de la información a corto, mediano y largo plazo.

4.4. Fortalecer la cultura institucional de seguridad digital.

5. ALCANCE

La presente Política es de obligatorio cumplimiento para todos los servidores públicos, contratistas, proveedores y terceros que tengan acceso a la información o a los recursos tecnológicos del Instituto, independientemente de su modalidad de vinculación o del medio de acceso utilizado.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

10. POLÍTICAS ESPECÍFICAS

10.1. Uso de dispositivos móviles: Se permite el uso de dispositivos institucionales o personales autorizados, siempre que se cumplan las medidas de seguridad definidas por la Entidad.

10.2. Uso de conexiones remotas: El acceso remoto deberá contar con autorización previa y mecanismos de autenticación segura.

10.3. Gestión de activos de información: Los líderes de proceso serán responsables de identificar, clasificar y proteger los activos de información.

10.4. Protección frente a software malicioso: La Entidad implementará mecanismos para prevenir, detectar y mitigar amenazas digitales.

10.5. Copias de respaldo: La información institucional contará con esquemas de respaldo que garanticen su recuperación.

10.6. Control de accesos: El acceso se otorgará bajo el principio de mínimo privilegio.

Dirigidas a: responsables de sistemas de información, soporte técnico o contratistas tecnológicos.

INSDEPORTES CAJICÁ deberá asegurar que los sistemas de información utilizados para la gestión institucional cumplan, como mínimo, con los siguientes lineamientos:

- Exigir autenticación obligatoria para el acceso a todos los recursos y operaciones ejecutadas mediante software institucional.
- Garantizar que no se almacenen contraseñas, credenciales, cadenas de conexión u otra información clasificada o restringida en texto claro, implementando mecanismos de cifrado y controles de integridad.
- Implementar controles que impidan la visualización de contraseñas durante su ingreso, almacenamiento o recuperación.
- Desarrollar o configurar el software institucional conforme a estándares de desarrollo seguro, privilegiando buenas prácticas de seguridad digital.
- Implementar controles que eviten múltiples intentos fallidos de autenticación, tales como bloqueos temporales o alertas de seguridad.
- Velar por la asignación controlada de privilegios de acceso, modificación y revocación en los sistemas de información.
- Monitorear periódicamente los perfiles de usuario y los privilegios asignados, verificando su coherencia con las funciones desempeñadas.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

Ingeniería social: Técnicas de manipulación para obtener información o accesos no autorizados.

Integridad: Protección de la exactitud y consistencia de la información.

Riesgo: Posibilidad de afectación negativa a la información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad.

Seguridad digital: Conjunto de medidas para proteger activos de información y servicios digitales.

Seguridad lógica: Controles tecnológicos de acceso y monitoreo.

Seguridad física: Medidas de protección de activos tecnológicos frente a accesos no autorizados.

Usuario: Persona que utiliza recursos tecnológicos de la Entidad.

Virus: Software malicioso que altera el funcionamiento de sistemas.

Vulnerabilidad: Debilidad susceptible de ser explotada por una amenaza.

8. PRINCIPIOS

La Política de Seguridad Digital se rige por los siguientes principios:

5.1. Confidencialidad
5.2. Integridad
5.3. Disponibilidad
5.4. Legalidad
5.5. Responsabilidad
5.6. Gestión del riesgo
5.7. Mejora continua

9. LINEAMIENTOS GENERALES

INSDEPORTES CAJICÁ adoptará, entre otros, los siguientes lineamientos:

a. Protección de los activos de información y datos personales.
b. Uso responsable y autorizado de los recursos tecnológicos institucionales.
c. Gestión de accesos y credenciales de usuario.
d. Prevención, detección y gestión de incidentes de seguridad digital.
e. Implementación de copias de seguridad y mecanismos de recuperación.
f. Concientización y cultura organizacional en seguridad digital.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

- Transportar y almacenar los equipos en lugares seguros y, cuando sea posible, utilizar mecanismos de sujeción o seguridad física.

- Evitar el uso de los equipos institucionales en lugares públicos sin las medidas de protección adecuadas.

- **Uso de aplicaciones y herramientas.**

  - Usar únicamente las aplicaciones colaborativas, plataformas de teleconferencia y herramientas digitales autorizadas por el Instituto.
  - Está prohibido el uso de programas, aplicaciones o servicios no controlados o no autorizados.
  - En actividades de videoconferencia se deberán aplicar las siguientes buenas prácticas.
  - Activar salas de espera y bloquear reuniones.
  - Permitir el acceso solo a participantes autorizados.
  - Evitar compartir información confidencial.
  - Informar previamente a los participantes si la reunión será grabada.

- **Prevención de riesgos digitales**
  - Evitar hacer clic en enlaces sospechosos.
  - Descargar archivos únicamente de fuentes conocidas.
  - No abrir correos de remitentes desconocidos.
  - Evitar el uso de redes sociales y aplicaciones de mensajería no corporativas para asuntos institucionales.
  - Evitar la navegación en sitios no seguros.
  - Evitar el uso de dispositivos de almacenamiento externo; en caso de utilizarlos, escanearlos previamente con software antivirus.

- **Uso de equipos personales**

  - Cuando se autorice el uso de equipos personales para trabajo remoto, el usuario deberá cumplir como mínimo con las siguientes condiciones
  - Mantener actualizado el sistema operativo.
  - Garantizar el correcto funcionamiento del equipo.
  - Contar con antivirus instalado, activo y actualizado.
  - Asegurar que el software utilizado cuente con licenciamiento válido, cuando aplique.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

- Verificar y ratificar semestralmente las autorizaciones de acceso a los recursos tecnológicos.

Revisar y validar toda creación, modificación o eliminación de perfiles de acceso a los sistemas de información del Instituto.

10.7. SEGURIDAD EN LAS COMUNICACIONES: Las redes y servicios de comunicaciones, así como las instalaciones que le dan soporte se gestionan y controlan para evitar accesos no autorizados. La información transmitida o transferida mediante redes públicas se salvaguarda a través de controles para prevenir la pérdida de confidencialidad, integridad y la pérdida de disponibilidad de estos.
La conexión de equipo o estaciones de trabajo a las redes del Instituto está controlada y supervisada.

10.8. TRABAJO REMOTO: dirigidas a: servidores públicos y contratistas que desarrollen funciones bajo modalidad remota o mixta.

Cuando se autorice el trabajo remoto, deberán observarse los siguientes lineamientos:

- **Seguridad de acceso y autenticación**

Configurar el inicio de sesión del equipo de cómputo con mecanismos de autenticación segura (contraseña, PIN o biometría).

No permitir el acceso a los sistemas institucionales desde redes públicas o no seguras; se recomienda el uso de redes cableadas o redes privadas confiables.

- **Manejo de la información**

Almacenar la información institucional únicamente en el servicio en la nube autorizado por el Instituto.

Proteger la información conforme a la clasificación de los activos de información.

Informar inmediatamente cualquier evento que pueda comprometer:

  - El equipo de cómputo,
  - La información,
  - Las credenciales de acceso,
  - Los sistemas de información,
  - Los medios de almacenamiento o las comunicaciones.

- **Protección física de los equipos**

  - Proteger físicamente los equipos institucionales utilizados para trabajo remoto, evitando su pérdida, daño o robo.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

- Asegurar que todo traslado físico de equipos institucionales cuente con autorización previa y documentada.
- Coordinar, cuando aplique, la existencia de pólizas de seguro para los equipos institucionales que deban ser trasladados o utilizados fuera de las instalaciones.
- Articular con el soporte técnico la asignación, reasignación o retiro de equipos tecnológicos conforme a la vinculación contractual o laboral.

10.9.4. Normas dirigidas a todos los usuarios

Todos los servidores públicos, contratistas y personal autorizado deberán cumplir las siguientes normas:

- La asignación, traslado, modificación o retiro de equipos tecnológicos solo podrá realizarse a través del Proceso de Gestión Administrativa y el soporte técnico autorizado.
  En consecuencia, se prohíbe cualquier disposición unilateral de los recursos tecnológicos institucionales.
- Los equipos asignados deberán ser utilizados exclusivamente para fines institucionales, conforme a las instrucciones técnicas suministradas.
- Ante cualquier falla o problema de hardware o software, el usuario deberá informar de manera inmediata al soporte técnico, sin intentar realizar reparaciones o modificaciones por cuenta propia.
- Está prohibida la instalación, reparación o retiro de componentes de hardware o software sin autorización del soporte técnico.
- Los usuarios deberán bloquear sus estaciones de trabajo al ausentarse de su puesto y apagar los equipos en horas no laborables o en ausencias prolongadas.
- Los equipos institucionales no deberán dejarse desatendidos en lugares públicos ni a la vista durante su transporte.
- El transporte de equipos deberá realizarse con las medidas de seguridad adecuadas, garantizando su integridad física.
- Los equipos portátiles deberán ser transportados como equipaje de mano, evitando su exposición a calor excesivo, humedad, impactos, campos electromagnéticos u otras condiciones que puedan dañarlos.
- En caso de pérdida o hurto de un equipo institucional, el usuario deberá informar de inmediato al líder del proceso y adelantar la denuncia ante la autoridad competente, conforme a los procedimientos internos.
- Al finalizar la jornada laboral, los usuarios deberán mantener sus escritorios libres de documentos con información institucional, asegurando su almacenamiento bajo las medidas de seguridad correspondientes.
- Está prohibido dejar visibles en pantalla documentos o información confidencial.

11. ROLES Y RESPONSABILIDADES

a. Dirección del Instituto: liderazgo y asignación de recursos para la implementación de la Política.
b. Procesos administrativos y misionales: cumplimiento de los lineamientos de seguridad digital.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
Mail: ventanillaunica@insdeportescajica.gov.co

10.9. SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

El Instituto Municipal de Deportes y Recreación de Cajicá con el fin de evitar la pérdida, robo, uso indebido o exposición al riesgo de los equipos de cómputo, dispositivos móviles y demás recursos tecnológicos institucionales, adopta la presente Política de Seguridad para los Equipos Institucionales, aplicable tanto dentro como fuera de las instalaciones de la Entidad.

La Entidad dispondrá de los mecanismos administrativos, técnicos y contractuales necesarios para mitigar los riesgos asociados a los recursos tecnológicos que soportan la gestión institucional, conforme a su estructura organizacional y a los servicios tecnológicos contratados.

10.9.1. El soporte técnico interno o el contratista tecnológico que haga sus veces deberá:

- Proveer e implementar mecanismos que garanticen la confidencialidad, integridad y disponibilidad de los recursos tecnológicos institucionales, tanto dentro como fuera de las instalaciones del Instituto.
- Definir y aplicar estándares de configuración segura para los equipos de cómputo y dispositivos tecnológicos utilizados por servidores públicos y contratistas.
- Establecer las condiciones mínimas de seguridad que deben cumplir los equipos de cómputo provistos por terceros que requieran conectarse a los sistemas o redes de la Entidad.
- Verificar el cumplimiento de dichas condiciones antes de conceder acceso a los servicios tecnológicos institucionales.
- Implementar controles diferenciados para los equipos que soportan procesos críticos o información sensible, con el fin de restringir accesos no autorizados.
- Atender, registrar y escalar los incidentes relacionados con fallas de hardware o software conforme a los procedimientos definidos.

10.9.2. Normas dirigidas al Proceso de Control Interno

El Proceso de Control Interno deberá:

- Evaluar la efectividad de los controles relacionados con la seguridad de los equipos institucionales.
- Analizar los informes, registros y evidencias sobre el uso, custodia y protección de los equipos de cómputo, especialmente en procesos críticos o de acceso restringido.
- Formular recomendaciones orientadas a fortalecer la gestión del riesgo asociado a los recursos tecnológicos, en el marco del MIPG.

10.9.3. Normas dirigidas a la Dirección

La dirección será responsable de:

- Verificar y controlar los ingresos y salidas de equipos de cómputo, dispositivos móviles y demás recursos tecnológicos de las instalaciones del Instituto.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

ANEXO 2
PLAN DE ACCIÓN – POLÍTICA DE SEGURIDAD DIGITAL

INSTITUTO MUNICIPAL DE DEPORTES Y RECREACIÓN DE CAJICÁ – INSDEPORTES CAJICÁ

Objetivo del Plan de Acción

Implementar de manera progresiva y articulada la Política de Seguridad Digital, fortaleciendo la gestión del riesgo digital, la protección de la información y la continuidad de los servicios institucionales.

Plan de Acción

Numeral Política	Lineamiento de la Política de Seguridad Digital	Actividad del Plan de Acción	Responsable	Apoyo / Ejecutor	Producto / Evidencia	Periodicidad	Dimensión MIPG	Rol Control Interno
	Control de accesos bajo principio de mínimo privilegio	Activar, modificar y desactivar accesos institucionales conforme a la vinculación contractual o laboral	Proceso de Gestión Administrativa	Soporte técnico / plataforma tecnológica contratada	Registros de activación y desactivación, matriz de usuarios y roles	Permanente	Control Interno / Gestión del Riesgo	Verificar correspondencia entre accesos y vigencia contractual
	Parametrización de perfiles y roles	Asignar perfiles y permisos según funciones y objeto contractual	Proceso de Gestión Administrativa	Soporte técnico	Perfiles configurados, trazabilidad de accesos	Permanente	Control Interno	Revisar segregación de funciones
	Uso seguro de dispositivos móviles	Autorizar y controlar el uso de dispositivos institucionales o personales autorizados	Dirección	Soporte técnico	Autorizaciones, lineamientos comunicados	Permanente	Control Interno	Validar cumplimiento de lineamientos
	Uso de conexiones remotas seguras	Controlar accesos remotos mediante autenticación y controles definidos	Proceso de Gestión Administrativa	Soporte técnico	Registros de accesos remotos	Permanente	Gestión del Riesgo	Verificar existencia de controles

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
Mail: ventanillaunica@insdeportescajica.gov.co

c. Proceso de Gestión Jurídica: evaluación jurídica, coherencia normativa y recomendaciones de mejora.
d. Proceso de Control Interno: verificación independiente conforme al esquema de líneas de defensa MIPG.
e. Comité Institucional de Gestión y Desempeño: seguimiento a la implementación de la Política.

12. Seguimiento

El seguimiento a la Política de Seguridad Digital se realizará en el marco de la Dimensión de Evaluación de Resultados del MIPG y estará a cargo del Comité Institucional de Gestión y Desempeño, mediante el análisis de indicadores, avances del Plan de Acción y reportes institucionales.

13. Evaluación

La evaluación de la Política estará a cargo del Proceso de Gestión Jurídica, con el acompañamiento del Proceso de Control Interno, conforme a la Dimensión de Control Interno del MIPG, verificando la legalidad, coherencia normativa, alineación institucional y efectividad de la Política.

La evaluación tendrá como propósito verificar la legalidad, coherencia normativa, pertinencia institucional y alineación jurídica de la Política con la Constitución, la ley, el Plan de Desarrollo Municipal, las políticas públicas sectoriales y los principios de la función administrativa.

Los resultados de la evaluación servirán como insumo para la mejora continua, la actualización de la Política y la adopción de acciones preventivas o correctivas, cuando a ello haya lugar.

10. Vigencia

La presente Política entra en vigencia a partir de la publicación del acto administrativo que la adopta y se mantendrá vigente mientras no sea modificada, actualizada o derogada por acto administrativo posterior.

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

Numeral Política	Lineamiento de la Política de Seguridad Digital	Actividad del Plan de Acción	Responsable	Apoyo / Ejecutor	Producto / Evidencia	Periodicidad	Dimensión MIPG	Rol Control Interno
	Gestión de activos de información	Identificar y clasificar activos de información por proceso	Líderes de proceso	Gestión Administrativa	Listado de activos clasificados	Anual	Gestión del Riesgo	Verificar identificación de activos
	Protección frente a software malicioso	Implementar mecanismos de prevención y detección de amenazas	Plataforma tecnológica contratada	Gestión Administrativa	Reportes de protección y monitoreo	Permanente	Gestión del Riesgo	Revisar existencia de controles técnicos
	Copias de respaldo de la información	Ejecutar y verificar copias de respaldo conforme a SLA	Plataforma tecnológica contratada	Gestión Administrativa	Registros de backups y restauración	Según SLA	Evaluación de Resultados	Verificar periodicidad y trazabilidad
	Seguridad de equipos institucionales	Controlar asignación, traslado y custodia de equipos institucionales	Proceso de Gestión Administrativa	Soporte técnico	Actas de entrega/recibo, inventarios	Permanente / anual	Control Interno	Cruzar inventario vs. asignaciones
	Protección física de equipos	Autorizar traslados y reportar pérdidas o hurtos	Proceso de Gestión Administrativa	Líderes de proceso	Autorizaciones, reportes de incidentes	Cuando ocurra	Gestión del Riesgo	Verificar acciones correctivas
Trabajo remoto	Seguridad en trabajo remoto	Socializar buenas prácticas de seguridad digital	Dirección del Instituto	Gestión Jurídica	Actas de socialización, circulares	Anual	Talento Humano	Verificar evidencia de capacitación
Incidentes	Gestión de incidentes de seguridad digital	Registrar y atender incidentes de seguridad	Gestión Administrativa	Soporte técnico	Reportes de incidentes, acciones tomadas	Cuando ocurra	Control Interno	Analizar causas y acciones
Seguimiento	Seguimiento de la Política	Realizar seguimiento a la implementación de la Política	Comité Institucional de Gestión y Desempeño	Planeación Estratégica	Informes de seguimiento	Anual	Evaluación de Resultados	Validar cumplimiento de acciones

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
E-Mail: ventanillaunica@insdeportescajica.gov.co

Numeral Política	Lineamiento de la Política de Seguridad Digital	Actividad del Plan de Acción	Responsable	Apoyo / Ejecutor	Producto / Evidencia	Periodicidad	Dimensión MIPG	Rol Control Interno
Evaluación	Evaluación independiente de la Política	Evaluar coherencia normativa, eficacia y controles	Control Interno	Gestión Jurídica	Informe de evaluación	Anual	Control Interno	Formular recomendaciones

Seguimiento del Plan de Acción

El seguimiento del presente Plan de Acción estará a cargo del Comité Institucional de Gestión y Desempeño, en el marco de la Dimensión de Evaluación de Resultados del MIPG, mediante el análisis periódico de indicadores, productos y avances registrados.

Evaluación del Plan de Acción

La evaluación del Plan de Acción será realizada por el Proceso de Gestión Jurídica, con el acompañamiento del Proceso de Control Interno, conforme a la Dimensión de Control Interno del MIPG, y servirá como insumo para la mejora continua y la actualización de la

Dirección: Calle 1 sur # 7 - 56.
Celular: (+57) 3133337759
www.insdeportes.gov.co
Mail: ventanillaunica@insdeportescajica.gov.co