

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 1 de 19
		Versión: 1

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2026

**Instituto Departamental de Deporte y Recreación de Bolívar
IDERBOL**

SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

VERSIÓN 1.0

Iderbol®

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 2 de 11
		Versión: 1

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

El Instituto Departamental de Deporte y Recreación de Bolívar (IDERBOL), en cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG) y las directrices establecidas en la Política de Gobierno Digital y la Política de Seguridad Digital, adopta estrategias y mecanismos que garanticen la protección, integridad, disponibilidad, confidencialidad y privacidad de la información institucional.

En el marco de la transformación digital, la seguridad de la información es un pilar esencial para que **IDERBOL** garantice servicios eficientes y confiables. El **Plan de Seguridad y Privacidad de la Información** surge para fortalecer la gestión de riesgos, establecer controles preventivos y consolidar una cultura organizacional basada en la confianza digital.

Respaldo por normativas como la **ISO/IEC 27001**, la Ley 1581 de 2012 y las directrices de MinTIC, este plan busca que funcionarios, contratistas y terceros adopten mejores prácticas de ciberseguridad. Para ello, se definen directrices para identificar amenazas y gestionar incidentes bajo el ciclo **PHVA (Planear-Hacer-Verificar-Actuar)**, asegurando la mejora continua.

Más que un mandato legal, este compromiso es clave para una gestión transparente. Su implementación permitirá a IDERBOL robustecer su gobernanza digital, proteger los activos institucionales y ofrecer servicios de alta calidad a la ciudadanía.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Fortalecer la confianza en los servicios de IDERBOL a través de un SGSI que garantice la privacidad y disponibilidad de la información. Bajo los lineamientos de la Política de Gobierno Digital y el ESPI, esta iniciativa mitiga riesgos cibernéticos y asegura una gestión institucional transparente y eficiente en beneficio de los deportistas y ciudadanos del departamento.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 3 de 11
		Versión: 1

1.2.2. OBJETIVOS ESPECÍFICOS

- Definir lineamientos y controles: Establecer un marco normativo interno que proteja los activos digitales de IDERBOL y garantice la continuidad operativa de los servicios institucionales.
- Fomentar la cultura de seguridad: Desarrollar estrategias de sensibilización y formación para funcionarios, contratistas y proveedores, promoviendo el uso responsable de las TIC y la protección de datos.
- Gestionar riesgos y amenazas: Identificar y mitigar vulnerabilidades mediante metodologías de análisis proactivo, asegurando una respuesta oportuna y efectiva ante incidentes o ciberataques.
- Garantizar el cumplimiento legal: Asegurar la observancia de la Ley 1581 de 2012, los Decretos 1078 de 2015 y 620 de 2020, y los estándares de la norma NTC-ISO/IEC 27001.
- Impulsar la mejora continua: Optimizar el SGSI mediante el ciclo PHVA (Planear-Hacer-Verificar-Actuar), fortaleciendo la resiliencia institucional frente a los desafíos tecnológicos.
- Robustecer la gobernanza de datos: Potenciar la interoperabilidad y el manejo seguro de la información para incrementar la transparencia y la confianza ciudadana en los servicios de deporte y recreación.
- Asegurar la resiliencia operativa: Implementar planes de respuesta y continuidad de negocio que permitan la operación ininterrumpida de los sistemas críticos ante cualquier contingencia.

Iderbol®

1.3. JUSTIFICACIÓN

En el marco de la transformación digital del sector público, la seguridad y privacidad de la información son pilares esenciales para garantizar la eficiencia y confiabilidad institucional. Como entidad rectora del deporte y la recreación en Bolívar, **IDERBOL** sustenta su operación en sistemas de información que facilitan la interacción con la ciudadanía; por ello, es imperativo implementar mecanismos robustos de ciberseguridad que protejan estos activos estratégicos.

La digitalización de trámites y servicios para los bolivarenses, si bien aumenta la eficiencia, también expone a la entidad a nuevas amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. Ante este escenario, **IDERBOL** adopta un enfoque preventivo y de gestión de riesgos, alineado estrictamente con las políticas de **Gobierno Digital**, el modelo **ESPI** y el marco normativo nacional (Ley 1581 de 2012 y Decretos 1078 de 2015 y 620 de 2020).

Este plan articula los esfuerzos institucionales para establecer controles y estrategias que mitiguen vulnerabilidades en nuestras plataformas tecnológicas. Su propósito es fortalecer la resiliencia ante incidentes de ciberseguridad, asegurando que las redes y servicios digitales operen bajo estándares de alta protección.

Asimismo, este documento sienta las bases para consolidar un **Sistema de Gestión de Seguridad de la Información (SGSI)**. A través de la implementación progresiva de respaldos, controles de acceso y protocolos de respuesta, buscamos no solo cumplir con la ley, sino arraigar una cultura organizacional de seguridad digital.

Finalmente, la ejecución de este plan beneficia directamente a la **Gerencia General y sus Subgerencias**, al proveer datos confiables para la toma de decisiones estratégicas. De igual forma, garantiza a la ciudadanía el acceso a plataformas seguras y ágiles, reafirmando el compromiso de **IDERBOL** con la transparencia y la excelencia en la prestación de sus servicios.

1.4. ALCANCE

El **SGSI de IDERBOL** integra un conjunto de medidas, controles y procesos diseñados para salvaguardar los activos de información institucionales. Su implementación garantiza el cumplimiento de los pilares de **confidencialidad, integridad, disponibilidad y privacidad**, bajo los estándares de la norma **NTC-ISO/IEC 27001:2022** y el marco legal vigente, incluyendo la Ley 1581 de 2012 y los Decretos 1078 de 2015 y 620 de 2020.

Este plan es de carácter vinculante para todos los funcionarios, contratistas y terceros que interactúen con la información de la entidad. Es responsabilidad de estos actores conocer y aplicar estrictamente las políticas y procedimientos establecidos. Para ello, se han definido controles específicos que protegen la infraestructura tecnológica, los sistemas de información, las bases de datos y cualquier componente físico o digital crítico para la gestión institucional.

Asimismo, el alcance del modelo contempla:

- **Gestión proactiva de riesgos:** Identificación y mitigación de amenazas digitales.
- **Resiliencia operativa:** Protocolos de respuesta efectiva ante incidentes de seguridad.
- **Cultura digital:** Programas continuos de capacitación y concienciación en ciberseguridad.
- **Evolución constante:** Aplicación del ciclo **PHVA (Planear-Hacer-Verificar-Actuar)** para asegurar la mejora continua de los procesos.

Mediante este enfoque integral, **IDERBOL** robustece su entorno organizacional, asegurando que la

información se gestione de manera segura y transparente. De esta forma, se garantiza la protección de los datos de los ciudadanos y la excelencia en la prestación de los servicios de recreación y deporte en el departamento.

2. MARCO CONCEPTUAL

El presente marco conceptual establece los términos y definiciones clave en el **Plan de Seguridad y Privacidad de la Información de IDERBOL**, en alineación con la **Política de Seguridad Digital** y la **Política de Gobierno Digital** del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Estas definiciones son fundamentales para la gestión de riesgos, el aseguramiento de la información y la implementación del **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en estándares internacionales como la **NTC-ISO/IEC 27001:2022**.

Aceptación del Riesgo

Decisión formal de asumir un riesgo residual dentro de los niveles aceptables definidos por la organización. Esta decisión se toma tras evaluar las medidas de mitigación y el impacto potencial sobre la operación y los activos de información.

Activo de Información

Cualquier recurso, tangible o intangible, que tiene valor para la organización y requiere protección. Esto incluye datos, sistemas de información, infraestructuras tecnológicas, documentos físicos o digitales, servicios y el conocimiento de las personas.

Alerta de Seguridad Digital

Notificación formal de un evento o incidente de seguridad que puede comprometer la confidencialidad, integridad o disponibilidad de la información y que requiere acciones inmediatas de mitigación.

Amenaza Digital

Causa potencial de un incidente de seguridad que puede ocasionar un impacto negativo en los sistemas de información, la infraestructura tecnológica o la continuidad de la operación.

Análisis de Riesgos

Proceso sistemático para identificar amenazas, vulnerabilidades y evaluar el impacto y la probabilidad de materialización de los riesgos que afectan la seguridad de la información.

Aplicaciones

Conjunto de programas o sistemas de software utilizados en la gestión de la información institucional y que deben cumplir con los estándares de seguridad digital.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 6 de 11
		Versión: 1

Autenticación

Proceso mediante el cual se verifica la identidad de un usuario, sistema o entidad antes de permitir su acceso a la información o recursos digitales.

Confidencialidad

Principio de seguridad que garantiza que la información solo esté disponible para personas, sistemas o procesos autorizados, previniendo accesos no autorizados o divulgación indebida.

Ciberespacio

Entorno digital compuesto por redes interconectadas, sistemas informáticos, dispositivos y servicios en línea donde se desarrolla la actividad digital de la sociedad, incluyendo la infraestructura tecnológica de IDERBOL.

Control de Seguridad de la Información

Medida implementada para mitigar riesgos, garantizar la protección de los activos de información y cumplir con las políticas y normativas aplicables.

Custodio del Activo de Información

Persona, cargo o unidad responsable de implementar y administrar los controles de seguridad definidos por el propietario del activo, asegurando su adecuada protección.

Datos Abiertos

Información pública, accesible y reutilizable sin restricciones, que promueve la transparencia y facilita la innovación y el desarrollo de servicios digitales.

Datos Biométricos

Información personal basada en características físicas únicas, como huellas dactilares, reconocimiento facial o voz, utilizadas para la autenticación e identificación de individuos.

Datos Personales Sensibles

Información que afecta la intimidad del titular y cuyo tratamiento indebido puede generar discriminación, incluyendo datos sobre origen racial, orientación política, religión, salud y biometría.

Disponibilidad

Propiedad de la información que garantiza que esté accesible y utilizable cuando se requiera por entidades o individuos autorizados.

Gestión de Incidentes de Seguridad Digital

Proceso estructurado para detectar, reportar, analizar y responder a incidentes de seguridad de la información, minimizando su impacto en la operación.

Gestión de Riesgos de Seguridad Digital

Conjunto de actividades para identificar, evaluar, tratar y monitorear riesgos de seguridad de la información, asegurando la continuidad de las operaciones y la protección de los activos digitales.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 7 de 11
		Versión: 1

Habeas Data

Derecho fundamental que garantiza el acceso, actualización y corrección de la información personal contenida en bases de datos, conforme a la **Ley 1581 de 2012** sobre protección de datos personales.

Incidente de Seguridad Digital

Evento inesperado que compromete la seguridad de la información y puede afectar la confidencialidad, integridad o disponibilidad de los activos digitales de la organización.

Integridad

Propiedad que garantiza la exactitud y confiabilidad de la información, evitando alteraciones o modificaciones no autorizadas.

No Repudio

Mecanismo de seguridad que impide que un usuario niegue haber realizado una acción o transacción digital, garantizando la trazabilidad y autenticidad.

Plan de Continuidad del Negocio

Estrategia que define las acciones necesarias para mantener la operación de la organización en caso de incidentes o crisis que afecten la seguridad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI)

Conjunto de políticas, procedimientos, recursos y controles implementados para gestionar la seguridad de la información de manera estructurada y alineada con la normativa vigente.

Trazabilidad

Capacidad de registrar y auditar todas las acciones realizadas sobre los activos de información, asegurando la rendición de cuentas y la seguridad en su gestión.

Vulnerabilidad

Debilidad en un sistema, procedimiento o control de seguridad que puede ser explotada por una amenaza, poniendo en riesgo la integridad de los activos de información.

3. MARCO NORMATIVO.

El Plan de Seguridad y Privacidad de la Información de **IDERBOL** se fundamenta en el bloque de constitucionalidad y la legislación colombiana vigente. Su cumplimiento garantiza la protección de los activos digitales, la privacidad de los ciudadanos y la integridad de la gestión pública.

3.1 Nivel Constitucional

Constitución Política de Colombia (1991): Especialmente el Artículo 15 (Derecho al Habeas Data y la intimidad) y el Artículo 20 (Derecho a la información y libertad de expresión).

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 8 de 11
		Versión: 1

3.2. Marco Legal (Leyes)

Ley 527 de 1999: Define y regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales.

Ley 594 de 2000 (Ley General de Archivos): Establece las reglas para la gestión documental, incluyendo el tratamiento de archivos electrónicos.

Ley 1273 de 2009 (Delitos Informáticos): Crea el bien jurídico tutelado de la protección de la información y de los datos, tipificando conductas criminales en el ciberespacio.

Ley 1341 de 2009 (Ley TIC): Marco general para el sector de las Tecnologías de la Información y las Comunicaciones.

Ley 1581 de 2012 (Protección de Datos Personales): Régimen general para el tratamiento de datos personales, fundamental para la privacidad en IDERBOL.

Ley 1712 de 2014 (Ley de Transparencia): Regula el acceso a la información pública y la gestión de la información mínima obligatoria.

3.3. Marco Reglamentario (Decretos y Resoluciones)

Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC): Compila las normas sobre la estrategia de Gobierno Digital en Colombia.

Decreto 620 de 2020: Establece los lineamientos para el uso y operación de los servicios ciudadanos digitales.

Resolución 500 de 2021 (MinTIC): Define los lineamientos y estándares para la seguridad, privacidad y el aprovechamiento de datos.

3.4. Instrumentos de Política (CONPES)

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, que actualiza las estrategias de respuesta ante amenazas cibernéticas.

CONPES 4019 de 2020: Política Nacional de Explotación de Datos (Big Data), que orienta el uso ético y seguro de la información.

3.5. Estándares Internacionales

NTC-ISO/IEC 27001:2022: Estándar internacional para los Sistemas de Gestión de Seguridad de la Información (SGSI), que sirve como base técnica para este plan.

4. ESTRATEGIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Estrategia de Seguridad y Privacidad de la Información

La estrategia de seguridad y privacidad de **IDERBOL** se fundamenta en la protección integral de sus activos digitales, alineándose con la Política de Seguridad Digital y el marco normativo colombiano. Su propósito central es salvaguardar la **confidencialidad, integridad y disponibilidad** de la información, fortaleciendo la gestión de riesgos y la protección de datos personales en todos los procesos institucionales.

1. Gestión de Riesgos y Diagnóstico

Se adoptará un enfoque proactivo basado en la metodología **MAGERIT**, complementado con estándares internacionales como **ISO/IEC 27001** y el marco de ciberseguridad **NIST**. El proceso iniciará con un diagnóstico exhaustivo para identificar y clasificar los activos digitales según su criticidad, seguido de un análisis de amenazas y vulnerabilidades que permitirá definir medidas de mitigación precisas.

2. Niveles de Implementación de Controles

La seguridad se estructurará en tres dimensiones estratégicas:

- **Nivel Técnico:** Implementación de cifrado de datos, autenticación multifactor (MFA), monitoreo de eventos de seguridad (SIEM) y segmentación de redes para prevenir accesos no autorizados.
- **Nivel Organizativo:** Adopción de políticas para el uso y tratamiento de datos, respaldadas por programas continuos de capacitación que consoliden una cultura de ciberseguridad en funcionarios y contratistas.
- **Nivel Normativo:** Aseguramiento del cumplimiento de la Ley 1581 de 2012, la Ley 1273 de 2009 y el Decreto 1078 de 2015, garantizando la transparencia en el manejo de la información pública.

3. Respuesta a Incidentes (CSIRT)

Se conformará un **Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)** bajo protocolos del estándar **NIST 800-61**. Este equipo garantizará la detección temprana de amenazas, una respuesta efectiva ante ataques y la recuperación ágil de los sistemas afectados, apoyándose en un sistema de reporte que impulse la mejora continua.

4. Privacidad desde el Diseño y Protección de Datos

La protección de datos personales se gestionará bajo el enfoque de **"Privacidad por Diseño"**, integrando la seguridad desde la creación de cada proceso. Se formalizará la figura del **Oficial de Protección de Datos**, encargado de supervisar el cumplimiento normativo, la gestión de consentimientos y la anonimización de información sensible cuando sea requerido.

5. Monitoreo, Evaluación y Mejora Continua

Para medir la eficacia de la estrategia, se establecerá un tablero de indicadores de desempeño (KPIs) que evaluará el nivel de madurez de la seguridad y la reducción de incidentes. Auditorías periódicas permitirán actualizar la estrategia frente a nuevos desafíos tecnológicos o cambios regulatorios.

4.1. PLAN DE ACCIÓN.

FASE	ACTIVIDADES	RESPONSABLES	PLAZO
Diagnóstico y evaluación de riesgos	Identificación de activos, análisis de amenazas y cálculo de riesgos	Asesor TIC, Planeación y Control Interno	3 meses
Implementación de Controles	Adopción de medidas técnicas y organizativas según ISO 27001	Asesor TIC, Subgerencia Administrativa y Financiera	6 meses
Gestión de Incidentes	Creación de protocolos de respuesta y formación del CSIRT	Asesor TIC	4 meses
Protección de Datos Personales	Implementación de políticas y designación de Oficial de Protección de Datos	Asesor TIC y jefe Jurídico	3 meses
Monitoreo y mejora continua	Auditorías, reportes de seguridad y actualización de planes	Asesor TIC, Planeación y Control Interno	Permanente

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 11 de 11
		Versión: 1

REFERENCIAS

Manual de Gobierno Digital – MINTIC.

Modelo de Seguridad y Privacidad de la Información – MINTIC.

CONPES No. 3701 del 2011 “Lineamientos de Políticas para la Ciberseguridad y Ciberdefensa”

CONPES No. 3854 de 2016 “Política Nacional de Seguridad Digital”

CONPES No. 3995 de 2020 “Política Nacional de Confianza y Seguridad Digital”

Decreto 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital” del Ministerio de las Tecnologías de la información y las Comunicaciones.

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5

Adicionalmente se utilizó IA mediante Prompts específicos guiados por la experiencia del Asesor TIC

CONTROL DE CAMBIOS.

Versión	Fecha y número de Acta y/o Acto Administrativo aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio
1	Acta Comité Institucional de Gestión y Desempeño No.001-2026	Erika Mejia	Edgardo Olarte, Steffi Chalave	Julio Morelos	Creación del documento.

