

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO DEPARTAMENTAL DE DEPORTES Y RECREACIÓN

AÑO 2023

1. PRESENTACIÓN

El Instituto Departamental de Deportes y Recreación de Bolívar “**IDERBOL**” reconoce la importancia de proteger los activos de información institucional dado que están expuestos a daños o modificaciones por parte de terceros. En la gestión de los procesos estratégicos, misionales y de apoyo del Instituto, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa que van desde un dato personal hasta secretos de los deportistas, asociaciones y usuarios que no deben ser divulgados a personal no autorizado, lo cual pondría en riesgo tanto al instituto o como la gestión pública.

Por esta razón **IDERBOL** asume el reto de implementar el Sistema de Gestión de la Seguridad de la Información (SGSI), de manera paulatina, de acuerdo con sus posibilidades estructurales, organizacionales y presupuestales, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la **Estrategia de Gobierno Digital**.

Somos conscientes que la defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de nuestros objetivos institucionales, y para cumplir con las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013 y en la Política de Seguridad Digital.

2. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.

El Instituto Departamental de Deportes y Recreación de Bolívar **IDERBOL**, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado en el Sistema de Gestión de Seguridad de la Información, debe proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información de valor, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes que afecten el desarrollo de la gestión institucional.

Proyectamos el desarrollo del componente de “**TIC**”, para una mayor protección, seguridad y privacidad de la información, orientado a la mejora continua y al eficiente desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo por el acceso, uso efectivo y apropiación masiva de las TICs, a través del diseño y ejecución de políticas y programas que mejoren la calidad de vida de los deportistas y ciudadanos que interactúan con Iderbol.

3. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.

Los objetivos de nuestra política de seguridad y privacidad de la información y de seguridad digital son:

-  Definir y adoptar marcos normativos para regular los temas de protección de la información.
-  Gestionar los riesgos de seguridad y privacidad de la información, y de seguridad Digital.
-  Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
-  Establecer mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información de Iderbol.
-  Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
-  Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de Iderbol.
-  Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información.

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

Aplica a todos los niveles jerárquicos y procesos del Instituto Departamental de Deportes y Recreación de Bolívar **IDERBOL**, a **todos sus funcionarios, contratistas, proveedores, operadores y** aquellas **personas o terceros** que en razón del cumplimiento de sus funciones y las de **IDERBOL**, compartan, utilicen, recolecten, procesen, intercambien o consulten su información; así como a los Entes de Control, y entidades que accedan, ya sea interna o externamente, a cualquier tipo de información, independientemente de su ubicación.

5. PLAN PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan para la implementación del Modelo de Seguridad y Privacidad de la Información se desarrollará a través del siguiente cronograma, al cual deberá hacersele seguimiento con carácter trimestral:

Componente	Actividades	Tareas	Responsable	Término
Activos de información	Revisar lineamientos para el levantamiento de activos de información	Definición de metodología e instrumento de levantamiento de activos de información		Enero de 2023
	Actualización del Inventario de Activos de Información	Recolección de información sobre activos de información		Marzo de 2023

		Gestionar los activos de información estableciendo la clasificación de la información (Pública, clasificada o reservada)		Marzo de 2023
Gestión del Riesgo	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos		Enero de 2023
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información.		Marzo de 2023
	Identificación de riesgos	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital		Abril de 2023
	Control de riesgos	Establecer los controles y términos para la administración de los riesgos de seguridad digital y seguridad y privacidad de la información		Abril de 2023
	Publicación	Publicación de la matriz de riesgos de protección y seguridad de la información y de seguridad digital		Mayo de 2023
	Seguimiento	Seguimiento a los planes de tratamiento y plan de seguridad y privacidad de la información	Control Interno	Trimestral
	Mejoramiento	Identificación de oportunidades de mejora y suscripción de planes de mejoramiento acorde con los resultados obtenidos en los procesos de evaluación	Todos los procesos	Permanente
	Procedimiento	Elaborar el procedimiento para regular los incidentes		Junio de 2023

Gestión de incidentes de la Seguridad de la Información	incidentes de seguridad de la información	de seguridad de la información		
	Socialización	Socializar el procedimiento de incidentes de seguridad de la información		Junio de 2023
	Gestionar los incidentes	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.		Permanente
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información		Junio de 2023
	Desarrollar la verificación	Dejar evidencias del cumplimiento de los Requisitos Legales de Seguridad de la Información		Junio de 2023
Planeación	Elaboración de Políticas y guías	Elaborar el Manual y/o Políticas de Seguridad de la Información		Marzo de 2023
MIPG	Gobierno Digital	Gestionar el autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información		Abril de 2023
	Ajustes	Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.		Mayo de 2023
	Política de seguridad digital	Revisar el avance de implementación de la política de Seguridad Digital en la Entidad		Mayo de 2023