

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

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024



**SUBDIRECCIÓN
ADMINISTRATIVA Y FINANCIERA**

VERSIÓN 1.0

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 2 de 7
		Versión: 1

Contenido

1. GENERALIDADES DEL PLAN INSTITUCIONAL	3
1.1. INTRODUCCIÓN.....	3
1.2. OBJETIVOS.....	3
1.2.1. OBJETIVO GENERAL	3
1.2.2. OBJETIVOS ESPECÍFICOS.....	3
2. CONTEXTO ESTRATÉGICO.....	4
3. MARCO CONCEPTUAL.....	4
4. MARCO NORMATIVO	5
5. DESCRIPCIÓN DEL PLAN	6
6. METODOLOGÍA DE SEGUIMIENTO.....	7
6.1. PLAN DE ACCION.	7
7. CONTROL DE CAMBIOS	7

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 3 de 7
		Versión: 1

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

El presente plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información se formula para promover en el Instituto Departamental de Deportes y Recreación de Bolívar IDERBOL, el compromiso de proteger la información que recibe gestiona y produce la entidad, para generar mayor confianza en ella por el adecuado tratamiento de la información que almacena.

El Instituto Departamental de Deportes y Recreación de Bolívar IDERBOL recibe, produce y gestiona información diariamente que resulta crucial para el correcto desempeño y cumplimiento de los objetivos institucionales, de ahí que la seguridad y la privacidad de la información revista tal importancia para la alta dirección. Buscamos evitar cualquier posibilidad de mal uso o pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios.

Como corolario de lo anterior, el proceso de gestión administrativa de la Instituto Departamental de Deportes y Recreación de Bolívar IDERBOL coordinará la implementación del mapa de riesgos de seguridad y privacidad de la información, y el monitoreo sobre las acciones establecidas para controlar o administrar los riesgos.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Fortalecer las capacidades institucionales para la Identificación, gestión, tratamiento y mitigación de los riesgos de Seguridad y privacidad de la información en las actividades institucionales en el entorno digital, en un marco de cooperación, colaboración y asistencia con los grupos de valor y grupos de interés

1.2.2. OBJETIVOS ESPECÍFICOS

- a) Gestionar los riesgos de seguridad y privacidad de la información, y de seguridad Digital.
- b) Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
- c) Generar conciencia para el cambio organizacional requerido para la
- d) Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 4 de 7
		Versión: 1

2. CONTEXTO ESTRATÉGICO

La Administración de riesgos de seguridad y privacidad de la información es un método metódico que nos permite identificar, analizar, evaluar, tratar, monitorear y trasladar los riesgos en respecto a la tecnología, equipos, infraestructura que almacenan y procesan datos de las operaciones de la entidad y datos personales de los usuarios que interactúan con nosotros, permitiendo minimizar pérdidas y maximizar oportunidades.

No hay que olvidar que toda infraestructura tecnológica que almacena datos está expuesta a daños, ataques cibernéticos u obsolescencia que representan un gran riesgo para las organizaciones, aunado a ello, afrontan dificultades por el mal uso que los administradores de los sistemas de información o bases de datos le dan a la información que almacena la entidad.

Para la administración del riesgo de seguridad y privacidad de la información en el Instituto Departamental de Deportes y Recreación de Bolívar IDERBOL se conciben tres elementos a saber: i) la Divulgación y apropiación de la política de seguridad y protección de datos personales de Iderbol ii) el Código de Integridad del Servidor Público y iii) la Política institucional de administración de riesgos de la entidad.

3. MARCO CONCEPTUAL

ACEPTACIÓN DEL RIESGO: Decisión de aceptar un riesgo. Activo: Según [ISO/IEC13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización.

ALERTA: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

AMENAZA: Según [ISO IEC13335-1:2004]: causa potencial de un incidente, el cual puede dar como resultado un daño a la entidad.

ANÁLISIS DE RIESGOS: Según [ISO IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

APLICACIONES: Es todo el software que se utiliza para la gestión de la información.

AUDITOR: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 5 de 7
		Versión: 1

AUDITORIA: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad de un proceso.

AUTENTICACIÓN: Proceso que tiene por objetivo validar la identificación de una entidad o sistema.

AUTENTICIDAD: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que manifiesta.

ESTÁNDAR: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

COMPROMISO DE LA ALTA GERENCIA: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de las políticas institucionales.

CONFIABILIDAD: la capacidad de un producto de realizar su función de la manera esperada.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

CONTROL CORRECTIVO: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

4. MARCO NORMATIVO

- CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- LEY 23 1982 Derechos de Autor.
- LEY 527 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 6 de 7
		Versión: 1

- LEY 594 2000 Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- LEY 603 2000 Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- LEY 962 2005 Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
- LEY 1150 2007 Seguridad de la información electrónica en contratación en línea.
- LEY 1266 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- LEY 1273 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- LEY 1341 2009 Por la cual se definen los 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 1474 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

5. DESCRIPCIÓN DEL PLAN

El resultado del diagnóstico de las condiciones de seguridad y de la administración del riesgo conlleva a un "Plan de seguridad y protección de la información" que debe contemplar las actividades a ejecutar para atender las debilidades extractadas de los diagnósticos, atender las oportunidades, optimizar las fortalezas y controlar los riesgos.

Para el diagnóstico de condiciones de seguridad y formulación del "Plan de seguridad y protección de la información" se deben observar el procedimiento de diagnóstico y el plan de acción de seguridad de la información con el formato de plan de acción correspondiente.

Adicionalmente, el Plan de acción de seguridad y protección de la información deberá integrarse al plan de procesos.

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

6. METODOLOGÍA DE SEGUIMIENTO

Para el correcto seguimiento del PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION de la Información al interior de la entidad, se construirán indicadores de gestión que permitirán establecer el avance de cumplimiento a partir de actividades planeadas para cada uno de los componentes que conforman el presente plan institucional.

Es de precisar que las actividades a desarrollar son apuestas al mejoramiento de los procesos dentro de la entidad en términos de transparencia, acceso a la información y lucha contra la corrupción.

6.1. PLAN DE ACCION.

Se estableció la herramienta Plan de Acción como criterio documental para la gestión del PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION ya que enmarca la hoja de ruta a seguir en la ejecución del plan.

Esta herramienta administrativa establece la ruta a implementar para gestionar los productos o metas necesarias para el cumplimiento de los objetivos en el marco de la misionalidad de la entidad.

7. 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. 001-2024	Steffi Chalave	Edgardo Olarte	Ariel Zambrano	Creación del documento.