

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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2024



**SUBDIRECCIÓN
ADMINISTRATIVA Y FINANCIERA**

VERSIÓN 1.0

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

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 2 de 19
		Versión: 1

Contenido

1. GENERALIDADES DEL PLAN INSTITUCIONAL	3
1.1. INTRODUCCIÓN.....	3
1.2. OBJETIVOS.....	4
1.2.1. OBJETIVO GENERAL.....	4
1.2.2. OBJETIVOS ESPECÍFICOS.....	4
2. JUSTIFICACIÓN	5
3. ALCANCE Y DELIMITACIÓN DEL PLAN.....	6
4. MARCO CONCEPTUAL	6
5. MARCO NORMATIVO	11
6. DESCRIPCIÓN DEL PLAN	12
7. DETALLE	12
8. METODOLOGÍA DE SEGUIMIENTO	12
8.1. PLAN DE ACCION.	13
9. CARACTERISTICAS PARA LA EJECUCIÓN DEL PLAN	17
10. CONTROL DE CAMBIOS	19

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 3 de 19
		Versión: 1

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

El Instituto Departamental de Deporte y Recreación busca garantizar el buen manejo de la información con la cual trabajara la organización por medio de los equipos, y demás herramientas tecnológicas con los cuales interactúan diariamente los funcionarios y usuarios en general, por consiguiente, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

La consecución de esto logrará que por medio de un Sistema de Gestión de Seguridad de la Información adoptada con normatividades nacionales e internacionales como la norma ISO 27001:2013, permita la evaluación de riesgos, el establecimiento de controles, la evaluación de la conformidad de las partes interesadas, tanto internas como externas y contribuirán en la ejecución de un plan de encadenamiento continuo de tratamiento de incidentes y de contingencia que son vitales para la institución, como medida preventiva ante cualquier eventualidad a la cual se pueda ver expuesta. Este Sistema de Gestión de Seguridad de la Información además permite el fortalecimiento de los procesos por medio del diseño, implementación y revaluación de la seguridad, lo cual arrojará como resultado el mejoramiento continuo gracias a la adopción del modelo PHVA (Planear-Hacer-Verificar-Actuar).

Para el instituto como institución de carácter público del orden territorial, cuyo objetivo principal es la de ofrecer servicios de recreación y deporte enfocados a mejorar el aprovechamiento del tiempo libre, y fortalecer el desarrollo personal de nuestra comunidad; propendiendo por el desarrollo sostenible de conformidad con las disposiciones normativas y legales, es importante y requerido para su operación el contar con un estándar de Seguridad de la Información, estándar que ayudará a mantener un sistema coherente con los procesos de la institución en beneficio de la comunidad.

Con la creación de objetivos claros y establecidos en la institución y las políticas aquí definidas brindaran las herramientas necesarias para que los funcionarios, contratistas y terceros que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI en adelante) del instituto, puedan adoptar los controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el SGSI, ello solo es posible a través de la integración de políticas, procedimientos, sistemas de información y controles con un fin común: gestionar de manera pertinente y eficaz los riesgos, de tal forma que las partes interesadas obtengan un alto nivel de seguridad y confianza.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 4 de 19
		Versión: 1

Se entiende, por lo tanto, que las políticas deben ser plenamente conocidas y cumplidas por los funcionarios, contratistas y terceras partes que tienen acceso a los activos de información y a los sistemas de procesamiento de información de IDERBOL. En este orden de objetivos, es indispensable que los esfuerzos y capacidades se concentren en lograr los fines primordiales de las políticas, como son: generar controles para proteger los activos de información; crear conciencia en los usuarios acerca del uso responsable de las tecnologías de la información y comunicaciones y realizar una gestión de riesgos adecuada que permita minimizar el impacto frente a un eventual caso de materialización.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de disponibilidad, confidencialidad e integridad al conjunto de datos y activos de información de IDERBOL.

1.2.2. OBJETIVOS ESPECÍFICOS

- a) Formular el esquema de seguridad de la información de acuerdo a las necesidades.
- b) Instaurar medidas de control de acceso a los activos de información de IDERBOL.
- c) Alinear a la normatividad vigente a nivel Nacional las políticas de gestión y administración de activos de información de la institución.
- d) Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información de IDERBOL.
- e) Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.
- f) Fortalecer la seguridad de la información, además de promover y mantener la confianza de los funcionarios, contratistas y terceros, mediante el desarrollo, implementación y cumplimiento de las políticas y procedimientos establecidos dentro del SGSI.
- g) Cumplir con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información de IDERBOL.
- h) Apoyar el cumplimiento de los principios de la función administrativa correspondientes a la legalidad, economía, eficacia, contradicción y publicidad, a través de los lineamientos establecidos por el SGSI.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 5 de 19
		Versión: 1

- i) Incentivar la cultura de la Seguridad y Privacidad de la Información fortaleciendo las buenas prácticas y la conciencia de los funcionarios, contratistas y terceros.
- j) Gestionar los riesgos de seguridad de la información con el fin de evitar el impacto en los objetivos estratégicos de IDERBOL, en especial, en aquellos que afecten los procesos misionales.
- k) Garantizar la continuidad del negocio mediante la implementación de planes y controles que sea necesario desarrollar frente a la existencia de incidentes de seguridad de la información.
- l) Apoyar las innovaciones y proyectos tecnológicos que garanticen los niveles de seguridad de la información previstos por la Institución.

2. JUSTIFICACIÓN

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener cualquier institución y/o organización, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo máspreciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial de una organización y en consecuencia necesita ser protegido adecuadamente. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Hoy en día las instituciones que manejen sistemas de información han generado la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno en Línea, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y los servicios tecnológicos de IDERBOL, se hace necesario levantar una línea de base sobre la cual se articulen diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

Es importante aclarar que este plan se encamina a formar las bases para una declaratoria de lineamientos progresivamente aplicables que vayan dando forma al Plan de Seguridad Informática partiendo desde las copias de seguridad, su

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 6 de 19
		Versión: 1

protección, integralidad, restricción de acceso y demás elementos a tener en cuenta.

Los principales beneficiarios son en primera medida la Alta Dirección, ya que se ofrecerá disponibilidad y veracidad en la información que se usa para la toma de decisiones. Por otra parte, los usuarios finales del sistema de información que alimentan y requieren de agilidad y seguridad al momento de ingresar información que puede o no ser pública, a través de los servicios tecnológicos de IDERBOL.

3. ALCANCE Y DELIMITACIÓN DEL PLAN

El objetivo que se busca con la implementación de su SGSI es mejorar los niveles de seguridad de la información y la protección de los activos de información, para lograrlo sabe que es indispensable implementar los controles según lo señalado por el estándar ISO 27001:2013 y la normatividad vigente aplicable.

Por tal razón, los funcionarios, contratistas y terceros que interactúen con los activos de información de IDERBOL, como ya se ha mencionado, deberán conocer y cumplir las políticas, procesos y procedimientos que hacen parte del SGSI, salvaguardando ante todo los principios de confidencialidad, integridad y disponibilidad que los protegen frente a cualquier tipo de tratamiento.

4. 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 institución.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 7 de 19
		Versión: 1

ACTIVO: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

AMENAZA INFORMÁTICA: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia)

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.

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 institución o sistema.

AUTENTICIDAD: Los activos de información solo pueden estar disponibles verificando la idinstitución de un sujeto o recurso, Propiedad que garantiza que la idinstitución 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 institución 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]:"

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 8 de 19
		Versión: 1

característica/propiedad por la que la información no está disponible o revelada a individuos, instituciones, o procesos no autorizados.

CIBERESPACIO: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

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.

CUSTODIO DE ACTIVO DE INFORMACIÓN: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Corporación, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la institución.

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.

DATOS ABIERTOS: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

DATOS BIOMÉTRICOS: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

DATOS PERSONALES SENSIBLES: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

DATO PÚBLICO: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 9 de 19
		Versión: 1

ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

DATO SEMIPRIVADO: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

DISCO DURO: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable cuando lo requiera una institución autorizada.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

GESTIÓN DE CLAVES: son controles que realizan mediante la gestión de claves criptográficas.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

GESTIÓN DE RIESGOS: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

HABEAS DATA: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

IMPACTO: el coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 10 de 19
		Versión: 1

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente.

La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

INTEGRIDAD: la propiedad de salvaguardar la exactitud y complejidad de la información.

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012).

NO REPUDIO: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

PARTE INTERESADA (STAKEHOLDER): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PLAN DE CONTINUIDAD DEL NEGOCIO: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o institución.

TRAZABILIDAD: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o institución.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 11 de 19
		Versión: 1

VULNERABILIDAD: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

5. 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 instituciones 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 instituciones de certificación y se dictan otras disposiciones.
- 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 instituciones 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.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 12 de 19
		Versión: 1

- 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.

6. DESCRIPCIÓN DEL PLAN

El Plan de seguridad es un documento que denota el compromiso de IDERBOL con la seguridad de la información. Este Plan contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la institución apoyadas en el uso adecuado de TICs.

7. DETALLE

EL INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DE BOLIVAR. debe salvaguardar las características de integridad, disponibilidad y confidencialidad de la seguridad de la información, mediante la adopción de políticas y procedimientos institucionales orientadas al logro de sus objetivos estratégicos, en estricto cumplimiento de las normas vigentes. De este modo, IDERBOL velará por la adecuada gestión de los riesgos, la adopción de buenas prácticas en el uso de los activos de información y la mejora continua de las competencias del talento humano.

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso de la Alta Dirección y la participación activa de los funcionarios, contratistas y terceros, quienes mancomunadamente deberán alcanzar el nivel de cumplimiento según los lineamientos y requisitos de seguridad de la información determinados aquí, así como el desarrollo de estrategias de mejora continua y gestión oportuna frente a incidentes o eventos de seguridad de la información.

8. METODOLOGÍA DE SEGUIMIENTO

El modelo por implementar es el ciclo PHVA, como metodología para la mejora continua.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 13 de 19
		Versión: 1

Además, se debe verificar la existencia de los siguientes lineamientos: planeadas para cada uno de los componentes que conforman el presente plan institucional.

8.1. PLAN DE ACCION.

Una vez la institución ha logrado alinearse con el SGSI entra en el ciclo PHVA	LINEAMIENTO 1. IDENTIFICAR EL NIVEL DE MADUREZ EN S.I
	FASE 1. Preparación
	Plan de capacitación Conformación Equipo de Gestión del Plan
	FASE 2. Análisis situación actual y definición de brechas.
	- Diseñar y aplicar encuesta de seguridad. - Definir nivel de madurez: Realizar autoevaluación con respecto a los niveles de seguridad. - Definición de brechas: Revisión de estructura organizacional. Revisión por niveles de madurez de acuerdo con los requisitos del manual. Revisión de controles de SI (Existentes y ausentes). Definir el estado actual de SI de la institución. Definición del plan o cronograma a seguir para disminuir la brecha y alinearse con el nivel de madurez adecuado.
	FASE 3. Alineación con el Sistema de Gestión de Seguridad de la Información SGSI.
	Ejecución del Programa para la reducción de la brecha.
PLANEAR	LINEAMIENTO 2. LLEVAR A LA INSTITUCIÓN A UN NIVEL DE MADUREZ INICIAL EN SEGURIDAD.
	FASE 1. Actividades Lineamientos Nivel Inicial
	Obtener soporte de la Dirección de la institución. Identificar legislación y normatividad aplicable.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 14 de 19
		Versión: 1

	Definir el alcance del SGSI “SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN” Definir la Política de la Seguridad de la información. Realizar el análisis de riesgo: Definir la aproximación para la Gestión del Riesgo. Realizar la identificación de Activos. Identificar los riesgos Analizar el riesgo en contexto de los objetivos de la institución y partes interesadas. Selección de Controles. Plan de Tratamiento del riesgo. Generar el DDA - Declaración de aplicabilidad.
	LINEAMIENTO 3. LLEVAR A LA INSTITUCIÓN A UN NIVEL DE MADUREZ BÁSICO EN SEGURIDAD. FASE 1. Actividades Lineamientos Nivel Avanzado. Implementar el plan de tratamiento del riesgo. Documentar los controles del SGSI: Definir métricas y medidas para medir el desempeño del SGSI. Implementar políticas y controles de seguridad de la fase de planeación. Implementar los planes de concientización y entrenamiento. Establecer y gestionar la operación del SGSI y sus recursos. Implementar la infraestructura de respuesta a incidentes.
	LINEAMIENTO 4. LLEVAR A LA INSTITUCIÓN A UN NIVEL DE MADUREZ AVANZADO EN SEGURIDAD. FASE 1. Actividades Lineamientos Nivel Avanzado. Ejecutar plan operacional. Revisiones regulares de eficacia: Monitorear y revisar políticas, estándares, procedimientos y prácticas. Revisar la eficacia de las operaciones de seguridad usando métricas y mediciones. Revisar el nivel del riesgo residual.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 15 de 19
		Versión: 1

	Realizar Auditorías internas. Realizar Auditorías externas. Revisión de la dirección del SGSI. Registro del impacto en el SGSI.
ACTUAR	LINEAMIENTO 5. LLEVAR A LA INSTITUCIÓN A UN NIVEL DE MADUREZ DE MEJORAMIENTO PERMANENTE EN SEGURIDAD.
	FASE 1. Actividades Lineamientos Nivel Mejoramiento Permanente.
	Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo. Tomar medidas preventivas y correctivas. Aplicar las lecciones aprendidas. Comunicar los resultados. -Proceso continuo y Gestión auto sostenible del modelo de las instituciones: Revisión de Política de Seguridad. Verificación del alcance del conjunto de políticas en la institución. Revisión de los activos de información de la institución. Revisión del riesgo residual. Recopilación y análisis de los indicadores del modelo. Análisis de estadísticas de incidentes de seguridad de la información en instituciones del Estado. Implementación de los ajustes.

Posterior a la revisión de cumplimiento de los lineamientos, se debe verificar el nivel de madurez del CGSI “Componente de Gestión de Seguridad de la Información”, de acuerdo con cómo se describe a continuación:

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 16 de 19
		Versión: 1

NIVEL	DESCRIPCIÓN
INEXISTENTE	Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad.
	No se reconoce la información como un activo importante para su misión y objetivos estratégicos.
	No se tiene conciencia de la importancia de la seguridad de la información en las instituciones
INICIAL	Se han identificado las debilidades en la seguridad de la información. - Los incidentes de seguridad de la información se tratan de forma reactiva.
	Se tiene la necesidad de implementar el MSPI “MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en el instituto; IDERBOL se encuentra en este nivel de madurez.
REPETIBLE	Se identifican en forma general los activos de información.
	Se clasifican los activos de información.
	Los servidores públicos de la institución tienen conciencia sobre la seguridad de la información.
	Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
ADMINISTRADO	La institución ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.
	La Institución ha determinado los objetivos, alcance y límites de la seguridad de la información.
	La Institución ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.
	La Institución tiene procedimientos formales de seguridad de la Información.
	La Institución tiene roles y responsabilidades asignados en seguridad y privacidad de la información.
	La Institución ha realizado un inventario de activos de información aplicando una metodología.
	La Institución trata riesgos de seguridad de la información a través de una metodología.
	Se implementa el plan de tratamiento de riesgos.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 17 de 19
		Versión: 1

OPTIMIZADO	En este nivel se encuentran las instituciones en las cuales la seguridad es un valor agregado para la organización.
	Se utilizan indicadores de efectividad para establecer si la institución encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

9. CARACTERISTICAS PARA LA EJECUCIÓN DEL PLAN

Se lleva a cabo una reseña de las principales características de la norma ISO/IEC 27001:2013, la cual se ha seleccionado como estándar para la implementación y mantenimiento del CGSI dentro de IDERBOL.

9.1 OBJETIVOS DE EJECUCIÓN.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN:

Establece la necesidad de definir un conjunto de políticas aplicadas a todas las actividades relacionadas con la gestión de la seguridad de la información dentro de IDERBOL, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:

Sugiere diseñar una estructura para la gestión de la seguridad de la información dentro la Organización que establezca los roles y responsabilidades con la seguridad de la información a lo largo de la misma.

SEGURIDAD DEL RECURSO HUMANO:

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan.

También determina cómo incide el papel que desempeñan los empleados como corresponsables de la seguridad de la información.

GESTIÓN DE ACTIVOS:

Detalla los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.

CONTROL DE ACCESO:

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 18 de 19
		Versión: 1

recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la Organización y el personal externo que brinda servicios, en concordancia con sus responsabilidades.

Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.

CIFRADO:

Garantiza el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.

SEGURIDAD FÍSICA Y AMBIENTAL:

Responde a la necesidad de proteger las áreas, los equipos y los controles generales.

El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la Organización, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.

SEGURIDAD DE LAS OPERACIONES:

Define las políticas, procedimientos y responsabilidades para asegurar la correcta operación de las instalaciones de procesamiento de información.

SEGURIDAD DE LAS COMUNICACIONES:

Define las políticas y procedimientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

Adquisición, desarrollo y mantenimiento de los sistemas de información: Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información. Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la Organización, para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.

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

RELACIÓN CON PROVEEDORES:

Permite asegurar la protección de los activos de información que son accedidos por proveedores.

GESTIÓN DE INCIDENTES DE SEGURIDAD:

Establece la necesidad de desarrollar una metodología eficiente para la generación, monitoreo y seguimiento de eventos e incidentes de seguridad.

Aspectos de seguridad de la información en la gestión de la continuidad del negocio: Considera el análisis de todos los procesos y recursos críticos del negocio, y define las acciones y procedimientos a seguir en casos de fallas o interrupción de los mismos, evitando la pérdida de información y la no disponibilidad de los procesos productivos de la Organización, lo que podría provocar un deterioro de la imagen de la Organización, una posible pérdida de clientes o incluso una dificultad severa que impida continuar operando.

CUMPLIMIENTO:

Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO/IEC 27001:2013, concuerda con otras leyes, reglamentos, normatividad y obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contrato de servicios, entre otros. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y las consideraciones técnicas; asimismo, busca garantizar que las políticas de seguridad y privacidad de la información sean acordes a la infraestructura tecnológica de la Organización.

10. 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.