PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO DE DEPORTES Y RECREACIÓN – INDER

GESTIÓN TECNOLOGICA
SUBDIRECCIÓN ADMNINISTRATIVA Y FINANCIERA

ENERO DE 2021

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

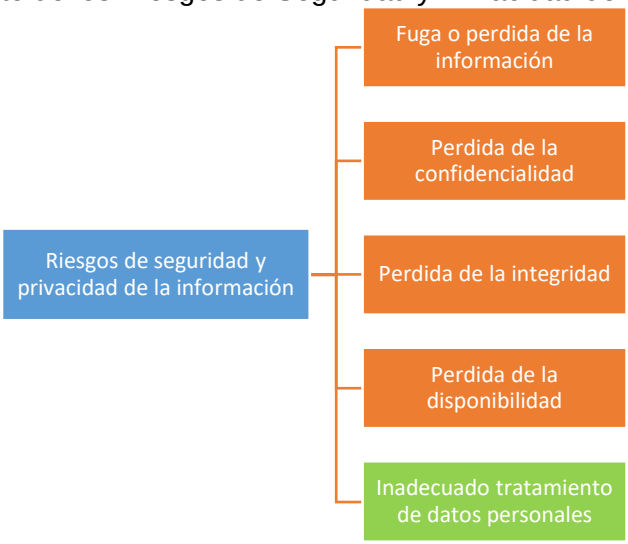
1. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información es crucial para el desarrollo del objeto misional del INDER Medellín, por tal razón debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

De acuerdo con lo anterior y tomando como referencia el Modelo de Seguridad y Privacidad de la información de MINTIC (MSPI), la gestión de riesgos de seguridad y privacidad de la información en el INDER Medellín cuenta con las buenas prácticas de las Norma Técnica Colombiana (ISO/IEC 31000, ISO/IEC 27005), la "Guía de Riesgos" del DAFP25, aprovechando el trabajo adelantado en la identificación de riesgos para ser complementados con los riesgos de seguridad y privacidad de la información.

1.1. Definición del Riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias". De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información del INDER Medellín, donde se busca diseñar una metodología ágil enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información.



1.2. Riesgos de Seguridad y privacidad de la información

Riesgos de seguridad de la información: Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. En la tipificación de dichos riesgos, se encuentran los siguientes:

a. **Fuga o Pérdida de la Información:** Información que hace que esta llegue a personas no autorizadas, sobre la que su responsable pierde el control o el estado que genera una condición irreparable en el tratamiento y procesamiento de la Información. Ocurre cuando un sistema de información o proceso diseñado para restringir el acceso sólo a sujetos autorizados revela parte de la información que procesa o transmite debido a errores en la ejecución de los procedimientos de tratamiento, las personas o diseño de los Sistemas de Información.
b. **Pérdida de la Confidencialidad:** Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.
c. **Pérdida de la Integridad:** Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
d. **Pérdida de la Disponibilidad:** Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Riesgos de Privacidad de la información: Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Como riesgo tipificado se cuenta con lo siguiente:

a. **Inadecuado Tratamiento de Datos Personales:** Uso no adecuado de la información que identifica a las personas, lo que repercute en una violación de los derechos constitucionales.

1.3. Incidente de Seguridad de la Información

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad”; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información.

1.4. Factores de Riesgo

Se entiende por factores de riesgo dentro del Subsistema de Seguridad de la Información, aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información del INDER Medellín. Entre los factores de riesgos que se encuentran identificados dentro de la entidad están los siguientes:

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.
Procesos	Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Condiciones generadas por agentes externos, las cuales no son controlables por la empresa y que afectan de manera directa o indirecta el proceso.

2. METODOLOGÍA DE ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1. Metodología de Valoración del Activo y Análisis de Riesgos de Seguridad de la Información

El INDER Medellín utiliza una metodología para valorar los riesgos de la Seguridad de la Información, basado en el Sistema de Gestión de Riesgos ya establecido en la entidad. La presente Guía Metodológica y la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyen al Sistema Integrado de Gestión abarcando los siguientes aspectos:

Se identifican los activos de información en el flujo de cada proceso, teniendo en cuenta las Tablas de Retención Documental, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociados a los factores.

En el esfuerzo de valoración del activo, se consideran los siguientes aspectos:

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional, Ofimática, Antivirus, Sistema Operativo (OS), Servidor de Terminales, Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales.

TIPO DE ACTIVOS	DESCRIPCIÓN
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos.
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Soportes de Información	**Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).
Claves Criptográficas	**Esenciales para garantizar el funcionamiento de los mecanismos criptográficos.** Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

La Valoración del Activo de Información se realiza mediante la identificación del impacto para el INDER Medellín por la pérdida de las propiedades, principios o fundamentos de la Seguridad de la Información, teniendo en cuenta la siguiente tabla de criterios:

Criterio	Valor
Crítico	= 5
Alto	= 3 y < 5
Medio	= 1 y < 3
Bajo	= 0 y < 1

Tabla # 2 Criterios

CONFIDENCIALIDAD: Impacto que tendría para el INDER Medellín, la pérdida de confidencialidad sobre el activo de información, es decir, que sea conocido por personas no autorizadas:

- **5. Crítico:** Es la existencia de información más crítica (Calificada, Vital o Esencial) a nivel de pérdida de su confidencialidad que cualquier otra y que por ende debe tener una mayor protección. A la información (Calificada, Vital o Esencial) sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al INDER.
- **4. Alto:** Es la información que es utilizada por los funcionarios del INDER para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al proceso evaluado y/u otros procesos del INDER.
- **3. Medio:** Es la información que es utilizada por los funcionarios del INDER para realizar sus labores en los procesos y que puede ser conocida por terceros con la autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al proceso evaluado y/u otros procesos del INDER.
- **2. Bajo:** Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada con ciertas restricciones dadas por el propietario del activo a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos del INDER. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo en los procesos del INDER.
- **1. Mínimo:** Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos del INDER. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo en los procesos del INDER.
- **0. Nulo:** Es la información que ha sido calificada como de conocimiento público y su divulgación no implica impacto negativo en los procesos del INDER.

INTEGRIDAD: Impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de la información y métodos de procesamiento fueran alterados.

- **5. Crítico:** La pérdida de exactitud y estado completo del activo impacta negativamente la prestación de servicios de tecnología y de información en el INDER.
- **4. Alto:** La pérdida en la exactitud de algún dato o estado del activo impacta negativamente la prestación de servicios de tecnología y de información en del INDER.
- **3. Medio:** La pérdida posible de en la exactitud de algún dato o estado completo del activo puede impactar negativamente al proceso que gestiona la información y/o a otros procesos del INDER.
- **2. Bajo:** La pérdida posible de en la exactitud de algún dato o estado completo del activo puede tener algún impacto negativo en los procesos del INDER.
- **1. Mínimo:** La pérdida de exactitud y estado completo activo no tiene ningún impacto negativo en los procesos del INDER.
- **0. Nulo:** La pérdida de exactitud y estado no genera situación negativa alguna en los procesos del INDER.

DISPONIBILIDAD: Impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

- **5. Crítico:** La falta o no disponibilidad de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en el INDER.
- **4. Alto:** La falta o no disponibilidad parcial de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en el INDER.
- **3. Medio:** La falta o no disponibilidad de algún dato que posea el activo de información o el mismo impacta negativamente al proceso que gestiona la información y/o a otros procesos del INDER.
- **2. Bajo:** La falta o no disponibilidad del activo de información en su componente puede tener algún impacto negativo en los procesos del INDER.
- **1. Mínimo:** La falta o no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos del INDER.
- **0. Nulo:** La falta o no disponibilidad de algún dato que posea el activo de información no afecta los procesos del INDER.

a. Se identifican los responsables y dueños de la información con base en la oficina o dependencia productora, así mismo se le asocian a su responsabilidad, el tratamiento de los riesgos de seguridad identificados.

b. Se consideran los factores de riesgo, las vulnerabilidades de los activos de información, las causas o amenazas que puedan determinar la materialización de un evento, sus posibles consecuencias o afectación, relacionándolos con la identificación del riesgo de seguridad o privacidad de la información. Todo lo anterior se realiza mediante la documentación de fuentes como: Entrevistas no estructuradas con los responsables de los activos y el desarrollo del flujo de la información en el proceso, fuentes estadísticas y tendencias de los riesgos de seguridad y privacidad, observaciones de expertos y analistas, estudio de los procedimientos, guías y diagramas de información, establecimiento de la criticidad del activo y su tratamiento por parte de las personas, los procesos y la tecnología, gestión de riesgos realizados anteriormente y detección de áreas o dependencias sensibles.

3. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

3.1. ACTIVIDADES

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.
    a. Entrevistar con los líderes del Proceso
4. Valorar del riesgo y del riesgo residual
5. Realizar matriz de riesgos de seguridad y privacidad de la información
6. Plantear al plan de tratamiento de riego aprobado por los lideres

3.2. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el INDER Medellín.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

3.3. CRONOGRAMA DE ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CRONOGRAMA DE ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2021

Actividad	Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar diagnóstico																																								
Realizar inventario de activos de información																																								
Elaborar alcance del Plan del Tratamiento de Riesgos de Seguridad y Privacidad de la información																																								
Realizar identificación de riesgos con los líderes de proceso																																								
Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información																																								
Valoración del riesgo residual																																								
Seguimiento y control																																								

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

El Plan de Tratamiento de Riesgos de Seguridad de la Información se integra a la presente Guía Metodológica y a la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyendo al fortalecimiento de los mecanismos de Gestión de Riesgos del Sistema Integrado de Gestión del INDER Medellín.

La formulación de actividades de tratamiento de riesgos de seguridad de la información y su aplicación de acuerdo con la valoración del riesgo inherente documentado, buscando integrar la implementación de la presente Guía Metodológica.

Elaborado por: Joaquin Londoño Silva	**Revisado y Aprobado por:** Luis Fernando Moreno Velez
Firma:	**Firma:**
Fecha: 30/01/2021	**Fecha: 30/01/2021**