PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INSTITUTO MUNICIPAL DE EDUCACIÓN FÍSICA, DEPORTE Y RECREACIÓNDE RIONEGRO – IMER

2024 – 2027

INDICE

INTRODUCCIÓN.

El Instituto Municipal de Educación Física, Deporte y recreación de Rionegro – IMER. Reconoce la información como un activo valioso y a medida que los sistemas de información apoyan cada vez más sus procesos misionales, se hace más necesaria la ejecución de planes, programas y proyectos que garanticen la integridad, confidencialidad y disponibilidad de la misma.

Debido a que la infraestructura de TI continuamente se encuentra expuesta a diferentes tipos de riesgos que podrían ocasionar pérdida o indisponibilidad de los sistemas de información, el Instituto Municipal de Educación Física, Deporte y recreación de Rionegro – IMER, y el área de sistemas, se encuentran comprometidos con este plan, con el fin de definir estrategias para responder de forma adecuada ante un evento, previniendo la materialización de riesgos, recuperando y/o restaurando los servicios informáticos en el menor tiempo posible reduciendo el impacto sobre los procesos críticos del instituto.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, el presente documento tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

OBJETIVO GENERAL

Orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo en el contexto de la seguridad y privacidad de la información, desde la identificación hasta el monitoreo; enfatizando en la importancia de la administración del riesgo.

OBJETIVOS ESPECÍFICOS

- Consolidar una administración de riesgos acorde con las necesidades del Instituto Municipal de Educación Física, Deporte y recreación de Rionegro – IMER. Como entidad Pública.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, a los servicios del Imer.

ALCANCE

Iniciar desde que se identifica el riesgo, por influencia de los agentes de origen interno o externo, que generan impactos negativos a las operaciones relacionadas con la infraestructura tecnológica, flujo de la información y servicios informáticos necesarios para la gestión del Instituto Municipal de Educación Física, Deporte y recreación de Rionegro – IMER, en el cumplimiento de su deber institucional. Finaliza con la implementación de las medidas de acción contempladas en el plan de contingencia**.**

MARCO NORMATIVO

NORMA	REFERNCIA
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones.
Ley 1712 de 2014	"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. (Modelo Integrado de Planeación y Gestión).
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Ley 1341 de 2009	Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones- TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Resolución MINTIC 746 de 2022	Del Ministerio de Tecnologías de la Información y las Comunicaciones, por el cual se fortalece el Modelo de Seguridad y Privacidad en la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
DOCUMENTO TÉCNICO EXTERNO 2016	Modelo de Seguridad y Privacidad de la Información – MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Versión 3.0.2, julio de 2016.
NTC / ISO 27001 2013	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

DEFINICION DE TÉRMINOS

TI: Sigla utilizada para las Tecnologías de la Información y son todas las tecnologías que permiten acceder, producir, guardar, presentar y transferir información. Gracias a estas, los campos de la educación, cultura, política, opinión y demás han logrado avanzar en la distribución y masificación de sus contenidos, planes de acción y trabajo y las diversas funcionalidades en sus áreas.

Seguridad informática: Campo de la informática encargado de la protección y vigilancia de la infraestructura computacional, la cual comprende software, bases de datos, metadatos, archivos y todos aquellos elementos que la organización considere pueden estar en riesgo, como por ejemplo la información confidencial. En esa medida, a través de un sistema de mantenimiento y seguridad se establecen una serie de protocolos y medidas que pretenden evitar cualquier tipo de amenazas las cuales pueden ser causadas por usuarios o programas maliciosos. (CCD, 2012).

Informática: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. (RAE, 2014).

Contingencia: Suspensión, interrupción, inesperada y no planificada de la disponibilidad de los recursos tecnológicos, en otras es “la posibilidad de que algo suceda o no suceda” (RAE, 2014).

Copia de Seguridad (Backup): Es el proceso de copia de seguridad con la finalidad de utilizarla para restaurar lo original después de una incidencia. De acuerdo a (ALESGA, 1998) es la copia total o parcial de información importante como respaldo frente a eventualidades. La copia de seguridad debería ser guardada en un soporte almacenamiento diferente del original, para evitar que un fallo en el mismo pueda estropear el original y la copia.

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Aceptación del riesgo: Es el nivel máximo de riesgo que la entidad está dispuesta a aceptar.

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…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000) Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC27000).

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Aceptación del riesgo: Es el nivel máximo de riesgo que la entidad está dispuesta a aceptar. 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…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC27000).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

MARCO REFERENCIAL

Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

El Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro-IMER, a través de su Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TI que contribuyen al desarrollo social y económico, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

CATEGORÍA	RESPUESTA AL RIESGO
Evitar el riesgo	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Aceptar el riesgo	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.
Reducir el riesgo	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.
Compartir el riesgo	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

Cada uno de los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento, de esta manera, poder realizar un análisis de los controles teniendo en cuenta el dueño del riesgo (responsable del proceso), ya que la definición de controles es el resultado del seguimiento y aplicación controles y de los cuales deben participar todos los interesados.

Para los riesgos de seguridad y privacidad de la información:

- El mapa de resumen de los riesgos de seguridad y privacidad de la información será presentado por el área de sistemas del Instituto, en el Comité de Gestión y Desempeño Institucional, con el fin que los directivos de la entidad tengan conocimiento de los mismos.

- El manejo de los riesgos de Seguridad y Privacidad de la Información cuyo nivel de riesgos residual se encuentre ubicado en zona de riesgo baja o moderada, podrá ser asumido por todas las áreas que manejan datos personales en el Instituto.

- Los riesgos de Seguridad y Privacidad de la Información cuyo nivel de riesgo residual se encuentre ubicado en zona de riesgo alta o extrema, deben contar con la aprobación del Instituto y sus directivos.

DESARROLLO DEL PLAN

A través del análisis de riesgo para activos de información permite, comprender claramente los riesgos a los que puede estar expuesto el Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro -IMER, por ello se hace necesario el que se tengan las técnicas necesarias que permitan identificar los riesgos específicos asociados a los activos y complementar este proceso de ser posible, con la identificación de aquellos puntos críticos de fallas.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro -IMER, guarda concordancia con la metodología emitida por el.

Metodología de Evaluación de Riesgos de Seguridad de la Información

La metodología de gestión de riesgos de seguridad de la información está alineada con la norma ISO/IEC 31000 y en la ISO 27005. Las actividades que hacen parte de la metodología, son las siguientes:

Identificación de riesgos

El objetivo de esta etapa es identificar los principales riesgos críticos a los cuales se encuentran expuestos los procesos de la Entidad. Los encargados de Riesgos identificarán, para los procesos de su responsabilidad, los riesgos críticos que pudieran afectar los objetivos y/o estrategias definidas para el área. Dicha identificación puede ser realizada a través de los siguientes métodos:

- Reuniones o con el equipo de trabajo.
- Encuestas a los distintos participantes del equipo de trabajo.
- Bases de datos o matices de riesgo de ejercicios previos.

Una vez Identificados los riesgos críticos, estos se deben documentar en una matriz de riesgos, clasificándolos por tipo de riesgo de acuerdo con lo siguiente:

Estratégico: Riesgo relacionado con los objetivos estratégicos, alineados con la misión de la Entidad.

De Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia el instituto.

Financieros: Riesgo relacionado con el uso eficaz y eficiente de los recursos financieros.

Operacional: Riesgo resultante de deficiencias o fallas en procesos, personas, sistemas o eventos externos.

Tecnológicos: Están relacionados con la capacidad tecnológica del IMER, para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Cumplimiento: Riesgo relacionado con el cumplimiento de leyes y regulaciones, especialmente concierne al cumplimiento de aquellas leyes y normas a las cuales el IMER, está sujeto.

VALORACIÓN DE LOS RIESGOS

El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos del Imer. Las debilidades de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los procesos del Instituto, deben ser identificadas y evaluadas teniendo en cuenta los criterios de evaluación definidos. En este proceso se debe realizar las siguientes actividades:

- Identificar el flujo de información de cada uno de los procesos
- Identificar las vulnerabilidades que existen en el proceso.
- Identificar las amenazas que podrían materializarse, dadas las vulnerabilidades existentes.
- Definir las escalas a utilizar

De acuerdo con los Lineamientos para la gestión de riesgos digital en entidades públicas emitida por el DAFP, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas

Se plantearán un listado de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos.

AMENAZA	TIPO
Polvo, corrosión	Evento natural
Inundación	Evento natural
Incendios	Evento natural
Fenómenos sísmicos	Evento natural
Perdida en el suministro de energía	Faño físico
Espionaje remoto	Acciones no autorizadas
Ingeniería social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Acceso forzado al sistema	Acciones no autorizadas
Manipulación de Hardware	Acciones no autorizadas
Manipulación de Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Sustracción de sistemas de información	Fallas técnicas

Identificación de Vulnerabilidades

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las áreas de trabajo	No existe un control para el acceso de las personas no autorizadas a ingresar a las oficinas
Falta de máquina trituradora de papel	La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos
Falta de equipos electrónicos para copias de respaldo	El no contar con un HDD externo, impide a los realizar copias de respaldo o Backups
Falta de equipos institucionales.	El no contar con suficientes equipos institucionales, lleva a los funcionarios a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y claves que pueden afectar al prestador.
Red	Tráfico sensible sin protección

Análisis del Riesgo de Seguridad de la Información

El análisis está basado en los flujos de información de cada uno de los procesos y los requerimientos de seguridad, tomando en cuenta los controles existentes. En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo.

Los criterios reflejarán los valores del Instituto, los objetivos y los recursos existentes.

NIVEL	PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
5	Siempre	El evento ocurrirá en la mayor parte de las circunstancias	Ocurre más de una vez al mes
4	Muy probable	Se espera que el evento ocurra en la mayor parte de las circunstancias	Ocurre más de una vez al año
3	Probable	El evento debe ocurrir en Algún momento	Ocurre menos de una vez al año
2	Poco probable	El evento debería ocurrir en algún momento	Ocurre más de una vez cada cinco años
1	Raro	El evento debe ocurrir, pero solo en circunstancias excepcionales	El evento ocurre rara vez

NIVEL	IMPACTO	DESCRIPCIÓN
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre el Instituto
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre el Instituto
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre el Instituto
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre el Instituto
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias mínimas sobre el Instituto

Estrategias en el tratamiento de riesgos

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

ESTRATEGIA	DEFINICIÓN
Transferir	Son procedimientos que permiten eliminar el riesgo por medio de la transferencia
Mitigar	Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.
Evitar	Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado
Aceptar	Consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información del Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro-IMER, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Teniendo en cuenta que, la seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, se alinea al componente de TI para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al

cumplimiento de la misión y los objetivos estratégicos de la entidad. Así como, apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, y otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

De acuerdo con esto, se definen las siguientes fases de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), estas permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

Fase de Diagnóstico - Etapas Previas a la Implementación

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Los procesos a identificar son:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Instituto.
- Identificar el nivel de madurez de seguridad y privacidad de la información del Instituto.
- Levantamiento de información la cual permite Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

Fase de Planificación

Luego de la obtención de la información a través del diagnóstico, el Imer, deberá proceder a elaborar el plan de seguridad y privacidad de la información en concordancia con el objetivo misional del instituto, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

Por medio del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información la Entidad puede definir los límites sobre los cuales se implementará la seguridad y privacidad en el Instituto. Este enfoque es por procesos y debe extenderse a toda el Imer.

Para determinar el alcance y los límites del plan, es importante tener en cuenta los procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

- Contexto del Instituto: que se puede entender cómo conocer la Entidad, necesidades y expectativas de las partes interesadas, y determinar alcance del MSPI.
- Liderazgo: es el compromiso de la alta dirección en la elaboración e implementación de la Política de Seguridad y privacidad de la información, así como de los roles, responsables y autoridades dentro del Instituto.
- Planeación: son las acciones para abordar los riesgos y oportunidades, así como el desarrollo de los objetivos y planes para lograrlos.
- Soportes: son los recursos, componentes, sensibilización, comunicación y documentación.

Fase de Implementación

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

- Control y Planificación Operacional.
- Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Definición de los Indicadores de Gestión.

Fase de Evaluación de Desempeño

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

- Monitoreo, análisis y evaluación.
- Auditoría interna
- Revisión por la alta dirección.
- Actividades