INSTITUTO MUNICIPAL DEL DEPORTE Y LA RECREACIÓN DE YUMBO - IMDERTY

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

YOAN URIEL SUÁREZ QUINTERO

GERENTE IMDERTY

ENERO – 2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Instituto Municipal del Deporte y la Recreación de Yumbo (IMDERTY) ha desarrollado una metodología orientada al mejoramiento continuo. Esta metodología tiene como objetivo identificar, analizar, evaluar, corregir, monitorear y dar a conocer los riesgos asociados al manejo de la información institucional. La finalidad es reducir los posibles impactos negativos causados por la pérdida, secuestro o manipulación malintencionada de la información.

El personal del área de Tecnologías de la Información (TI) desempeña funciones cruciales en la captura, procesamiento y reporte de información a través de herramientas tecnológicas. Además, facilita la intercomunicación entre usuarios externos e internos de la red. Esta interconexión directa hace que la empresa sea vulnerable a posibles ataques malintencionados o manipulaciones indebidas de la información, lo que podría acarrear problemas económicos, legales y administrativos.

Por este motivo, este documento se enfoca en establecer una línea de trabajo que permita al IMDERTY superar y/o reducir los riesgos asociados a la seguridad de la información, asegurando así la integridad y confidencialidad de sus datos.

2. OBJETIVOS

2.1. Objetivo general

Implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información el cual permita controlar, minimizar y erradicar los riesgos de seguridad y evitar de esta manera la perdida de información o datos de los procesos, servicios o personas.

2.2. Objetivos específicos

- Diagnosticar de la situación actual de la empresa en materia de riesgos de seguridad y privacidad de la Información.
- Implementar la Política de Seguridad Digital de la institución.
- Implementar controles y acciones encaminadas a prevenir y administrar los riesgos.
- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y MinTIC para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Optimizar y hacer uso de los recursos económicos y tecnológicos de la institución en la aplicación del Programa de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

3. DIRECCIONAMIENTO ESTRATÉGICO

Misión de TI: Utilizar las Tecnologías de la Información y Comunicaciones de manera innovadora y efectiva para optimizar la gestión, promoción y acceso a las actividades deportivas y recreativas. Nuestra misión es aprovechar las TIC para facilitar la participación ciudadana, mejorar la eficiencia operativa y enriquecer la experiencia deportiva, contribuyendo al bienestar y desarrollo integral de la comunidad.

Visión de TI: Convertirnos en un referente a nivel local en la integración de Tecnologías de la Información y Comunicaciones para el fomento del deporte y la recreación. Buscamos liderar la innovación digital en el ámbito deportivo, proporcionando plataformas tecnológicas avanzadas que promuevan la participación de la comunidad, la eficiencia en la gestión y la creación de experiencias enriquecedoras para todos los usuarios, contribuyendo así al desarrollo integral y saludable de la sociedad.

Alcance

El Plan Estratégico de Tecnologías de Información y Comunicaciones (PETIC), busca generar estrategias que lleven a la correcta implementación de proyectos de TI de acuerdo con el marco de referencia de MinTIC, el cual hace parte de la planeación estratégica del Instituto y pretende desarrollar los siguientes puntos:

- Un portafolio de Proyectos de TI.
- Modelo de Gestión de TIC.
- Modelo de Gobierno de TIC.
- Definición de los diferentes Planes transversales al PETIC como el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Plan Estratégico de Tratamiento Riesgos de Seguridad y Privacidad de la Información.

2.1. Misión

Promover la práctica de la educación física, el deporte, la recreación y el aprovechamiento del tiempo libre, contribuyendo al desarrollo humano integral y el mejoramiento de la calidad de vida de los habitantes del municipio de Yumbo.

2.2. Visión

Posicionar al municipio de Yumbo como modelo deportivo departamental y nacional reconocido por sus valores humanos y los logros en educación física, deporte, recreación y aprovechamiento del tiempo libre.

4. MARCO NORMATIVO

El presente Plan Estratégico en Tecnologías de Información y Comunicaciones (PETIC) está regido por las siguientes Leyes, decretos y lineamientos de orden nacional y territorial que sirven como parámetro y guía para el desarrollo adecuado del plan:

- **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.
- **Decreto 415 de 2016 Artículo 2.2.35.3:** Objetivos del fortalecimiento institucional.
- **Decreto 1078 de 2015 Artículo 2.2.5.1.2.2**: Instrumentos - Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
- **Ley 1712 de 2014:** Ley de trasparencia y de acceso a la información pública nacional.
- **Decreto Nacional 2573 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- **Directiva Presidencial No. 04 de 2012:** Eficiencia Administrativa y Lineamentos de la Política de Cero Papel en la Administración Pública.
- **Decreto 019 de 2012:** Ley anti-trámites.
- **Decreto 2693 de 2012:** Lineamientos generales de la estrategia de gobierno en línea para la Nación.
- **Ley 1474 de 2011:** Ley anticorrupción.
- **Ley 1273 de 2009:** De la protección de la información y los datos.
- **Decreto 1151 de 2008:** Mediante el cual se establecen los lineamientos generales de la Estrategia de Gobierno En Línea, que son de obligatorio cumplimiento para las entidades que conforman la administración pública en Colombia.
- **Ley 962 de 2005:** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2482 de 2012:** Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión.
- **Decreto Ley 019 de 2012:** Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Ley 1437 de 2011:** Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- **Ley 1341 de 2009:** Por la cual se definen 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 527 de 1999:** Por 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.
- **Documento CONPES 3920 de 2018:** Política Nacional de Explotación de Datos (Big Data)
- **Decreto 1413 de 2017:** Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 849 de 2016:** Por el cual se modifica la estructura del Departamento Administrativo de Ciencia, Tecnología e Innovación – COLCIENCIAS.
- **Documento CONPES 3854 de 2016:** Política Nacional de Seguridad Digital
- **Decreto 415 de 2016:** Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- **Ley 1753 de 2015:** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país".
- **Decreto 1083 de 2015:** Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).
- **Decreto 1078 de 2015:** Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea.
- **Decreto 103 de 2015:** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 en lo relativo a la gestión de la información pública y se dictan otras disposiciones.
- **Ley 1712 de 2014:** Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

5. CONCEPTOS ASOCIADOS

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la Agencia.

Administración del riesgo: Es un conjunto de elementos que brindan a la entidad la capacidad de realizar las acciones necesarias con el fin de disminuir, tratar y corregir el riesgo. (DAFP, 2009)

Activo de Información: Un activo de información es cualquier tipo información o elemento de valor que genere datos e información que se puede manejar en los diferentes procesos de la Organización.

Análisis de riesgos: Es un proceso de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a las medidas de un peligro o amenaza determinada.

Amenaza: Es la causa potencial de una situación de incidente y no deseada. (RAE).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias para determinar el grado en el que se cumplen cierto criterios o normas. (ISO/IEC 27000).

Causa: Es toda aquella fuente generadora de eventos (riesgos).

Ciberseguridad: Capacidad para minimizar el nivel de riesgo al que están expuestos los ciudadanos, las aplicaciones, los servicios y sistemas, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica y la informática. (CONPES).

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (RAE)

Consecuencia: Resultado de un evento. (RAE)

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo, para determinar si son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico. (RAE)

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de un riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

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. (ISO/IEC 27000).

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Integridad: Propiedad de la información relativa a su exactitud y completitud. (RAE)

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados. (RAE)

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida. (RAE)

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos de información o grupos de activos de información causando así daño a la organización.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular

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).

Tratamiento del Riesgo: Proceso para modificar el nivel de riesgo o nivel de ocurrencia de este.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos interrelacionados interactuantes que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

6. COMPONENTES DEL PLAN

Descripción del Plan

Como se ha mencionado durante todo el documento, este programa tiene como objetivo principal, la identificación, corrección y prevención de riesgos e incidentes de seguridad y privacidad de la información, por tal motivo se especificarán cada uno de los procesos dentro del proceso de gestión de riesgos.

6.1. Identificación del riesgo

El proceso de identificación del riesgo consiste en determinar que podría causar una perdida potencial de información, sistemas o servicios, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida.

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

6.2. Descripción de Causas

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

6.3. Consecuencias

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Pérdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

6.4. Valoración del Riesgo

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración:

6.5. Tratamiento, Seguimiento Y Control

Una vez identificado y valorados los riesgos, se prosigue a describir los controles o barreras a ser implementadas que fortalezcan los procesos, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del riesgo.

7. REFERECIAS

- Mintic – MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (2016) – Extraído en diciembre de 2019 http://www.mintic.gov.co/ - http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

- Mintic – MODELO DE SEGURIDAD (2018) – Extraído en diciembre de 2019 - http://www.mintic.gov.co/ - http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- ANI – PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - https://www.ani.gov.co/ - https://www.ani.gov.co/plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad-de-la-informacion

- Min Ciencias – TRATAMIENTO (2019) – Extraído en diciembre de 2019 - https://minciencias.gov.co - https://minciencias.gov.co/quienes_somos/planeacion_y_gestion/tratamiento

- ISO Tools - ISO27001 (2013) – Extraído en diciembre de 2019 - https://www.isotools.org - https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

- RuleWorks – The Risk Management Guide – Extraído en diciembre de 2019 - http://www.ruleworks.co.uk - http://www.ruleworks.co.uk/riskguide/

- Protejete – Matriz de Riesgo (2011) – Extraído en diciembre de 2019 - https://protejete.wordpress.com - https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

- ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. ISO/IEC 27001:2005, Tecnología de la Información – Técnicas de seguridad - Sistemas de gestión de Seguridad de la información – Requerimientos – Extraído en diciembre de 2019 - http://www.acis.org.co - http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

- ESCUELA DE INGENIERÍA DE ANTIOQUIA - Los sistemas en la planificación municipal - Extraído en diciembre de 2019 – http://revista.eia.edu.co - http://revista.eia.edu.co/articulos4/Art%202%20N4.pdf

- GISWIN. Fundamentals of Geographic Information System. (2010) - Extraído en diciembre de 2019 - http://giswin.geo.tsukuba.ac.jp - http://giswin.geo.tsukuba.ac.jp/sis/tutorial/FundamentalsofGIS_Estoque.pdf

- Departamento Administrativo de la Función Pública - Guía para la Administración del Riesgo (2018) - Extraído en diciembre de 2019 - https://www.funcionpublica.gov.co - https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

ELABORO Y REVISÓ: SANDRA V. TOBAR GARCÍA	**CARGO:** SUBGERENTE ADMINISTRATIVA Y FINANCIERA	**FIRMA:**
APROBÓ: YOAN U. SUÁREZ QUINTERO	**CARGO:** GERENTE	**FIRMA:**