Contenido

1. INTRODUCCIÓN

Instituto Municipal de Educación para el Trabajo y Desarrollo Humano de Yumbo – IMETY en busca del mejoramiento continuo desarrollo una metodología que permite identificar, analizar, evaluar, corregir, monitorear y dar a conocer los riesgos asociados al manejo de la información institucional, para disminuir la afectación que la perdida, secuestro o manipulación mal intencionada pueda causar en la empresa. Dentro de las actividades diarias del personal TIC se encarga de la captura, procesamiento y reporte de información mediante las herramientas tecnológicas, así como de intercomunicar los usuarios externos de la red con los usuarios internos, lo que implica de manera directa que la empresa sea completamente vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la empresa sortear y/o disminuir los riesgos que la rodean y lograr que su información este segura.

2. OBJETIVOS

OBJETIVO GENERAL

Desarrollar un programa 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.

OBJETIVOS ESPECÍFICOS

Diagnosticar de manera acertada y real la situación actual de la empresa en materia de riesgos de seguridad y privacidad de la Información.

Fomentar el uso y apropiación de la Política de Seguridad vigente en el personal de la empresa.

Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de 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. ALCANCE

El presente documento está enfocado en mejorar la estrategia para el análisis, diseño, ejecución y control de los riesgos, generados en las actividades cotidianas por el uso frecuente de información en IMETY

La corrección y prevención de los riesgos debe ser establecida bajo un proceso estructurado y sistemático es por ello por lo que este programa contiene la definición de los roles y responsabilidades. Adicionalmente se debe tener en cuenta los indicadores y parámetros de cada uno de ellos.

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de la empresa, a cualquier sistema de información o aspecto particular de control, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

4. DEFINICIONES

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).

5. MARCO NORMATIVO

A continuación, se enumeran todos los documentos, normas y/o leyes, que sirven de marco de referencia y base para la elaboración de este documento:

Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública

Ley 57 de 1985 -Publicidad de los actos y documentos oficiales

Ley 594 de 2000 - Ley General de Archivos

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos Pagina 7 de 13

Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública

Decreto 2364 de 2012 - Firma electrónica

Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos

Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales

Ley 527 de 1999 - Ley de Comercio Electrónico

Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley Estatutaria 1581 de 2012 - Protección de datos personales

Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información

6. DESCRIPCIÓN DEL PROGRAMA

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.

7. 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.

8. 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.

9. 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.

10. 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:

11. 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.

12. BIBLIOGRAFÍA

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

REVISO: INGMART	**CARGO:** CONTRATISTA	**FIRMA:**
APROBO: RUBEN DARIO MILLAN	**CARGO:** DIRECTOR	**FIRMA:**

ANEXOS

Anexo A. Control de Cambios

Versión	Fecha (dd/mm/aaaa)	Revisado por:	Aprobado por:	Descripción de la actualización
01	17/01/2019	Manuel Alberto Torres	Carlos Arturo Tello Becerra	Creación del Plan
02	28/06/2019	Christian Valencia	Carlos Arturo Tello Becerra	Modificación del plan se incluye definiciones y metodología
03	30/01/2020	Ruben Barreto/ Johana Orejuela	Jaime Sánchez Lenis	Se actualiza del objetivo riesgos de la metodología, matriz de calificación se incluye presupuesto y medición del modelo

04	27/01/2021	Jhon Jairo Ortiz	Jaime Sánchez Lenis	Modificación del objetivo del plan, inclusión de definiciones, condiciones generales, clasificación de los activos de información, oportunidades de mejora, recursos e indicadores.
05	23/09/2021	Ruben Barreto	Jaime Sánchez Lenis	Modificación del plan la periodicidad para realizar seguimiento será cuatrimestral.
06	24/01/2022	Claudia Vélez Arias	Jaime Sánchez Lenis	Modificacion
06	30/01/2023	Ruben Dario Barreto	Ruben Dario Millan	Se usa nueva guía de la función pública y se cambian fechas para la administración de los riesgos y establecer controles en el año 2023.
07	01/11/2023	Jose Cristian Valencia	Ruben Dario Millan	Se realiza actualización del plan para la vigencia 2024