INSTITUTO MINICIPAL DE CULTURA DE YUMBO

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

EQUIPO COLABORADOR

GESTIÓN DE DIRECCIÓN Y PLANEACIÓN

MANTENIMIENTO Y ADMINISTRACIÓN DE BIENES

ENERO 29 DE 2021

PABLO DANIEL PATIÑO QUIJANO
GERENTE

Gerente: Pablo Daniel Patiño Quijano
Reviso y aprobó: Comité de Gestión y Desempeño
Elaboró: Equipo de trabajo Planeación y Mantenimiento y Administración de Bienes.

INTRODUCCIÓN

El plan de tratamientos de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, en el cual se planean y se establecen las medidas necesarias para el tratamiento de riesgos de seguridad y privacidad de la información a desarrollar e implementar durante la vigencia 2021, en el Instituto Municipal de Cultura de Yumbo.

Con el desarrollo de este plan se permitirá la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos, dando a conocer aquellas situaciones que puedan comprometer en cumplimiento de los objetivos trazados por la entidad y de esta manera reducir la afectación o impacto de su materialización.

Lo anterior dando cumplimiento a la normativa por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el Decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la Guía para la Administración del Riesgo y Diseño de Controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital – Versión 4 emitida por el DAFP.

Es importante mencionar que el DAFP al final de la vigencia 2020 genero la actualización de la Guía para la Administración del Riesgo y Diseño de Controles en entidades públicas Versión 5. A través de la cual la entidad y el equipo de trabajo responsable de esta gestión, deberá tener en cuenta para aplicar dichos lineamientos una vez sea socializada por el DAFP en sus ajustes representativos para dar el respectivo tratamiento a este tipo de riesgos identificados en la entidad.

OBJETIVO

Identificar y analizar los Riesgos de Seguridad y Privacidad de la información del IMCY con las pautas necesarias para desarrollar y fortalecer una adecuada gestión, a través de controles y métodos que faciliten la determinación, la identificación de riesgo, oportunidades, análisis, la valoración y expedición de políticas, así como el seguimiento. De esta forma se busca que mediante el Tratamiento de Riesgos de Seguridad y Privacidad de la Información haya una mayor confianza en la información que se almacena y maneja en la Entidad.

ALCANCE

Este Modelo es aplicable a cualquier sistema de información o aspecto particular de control del IMCY, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información.

VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

DESCRIPCIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Los riegos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso. “Integridad, confidencialidad o disponibilidad”.

Para el riesgo identificado se debe asociar el grupo de activos o activos específicos del proceso y, conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

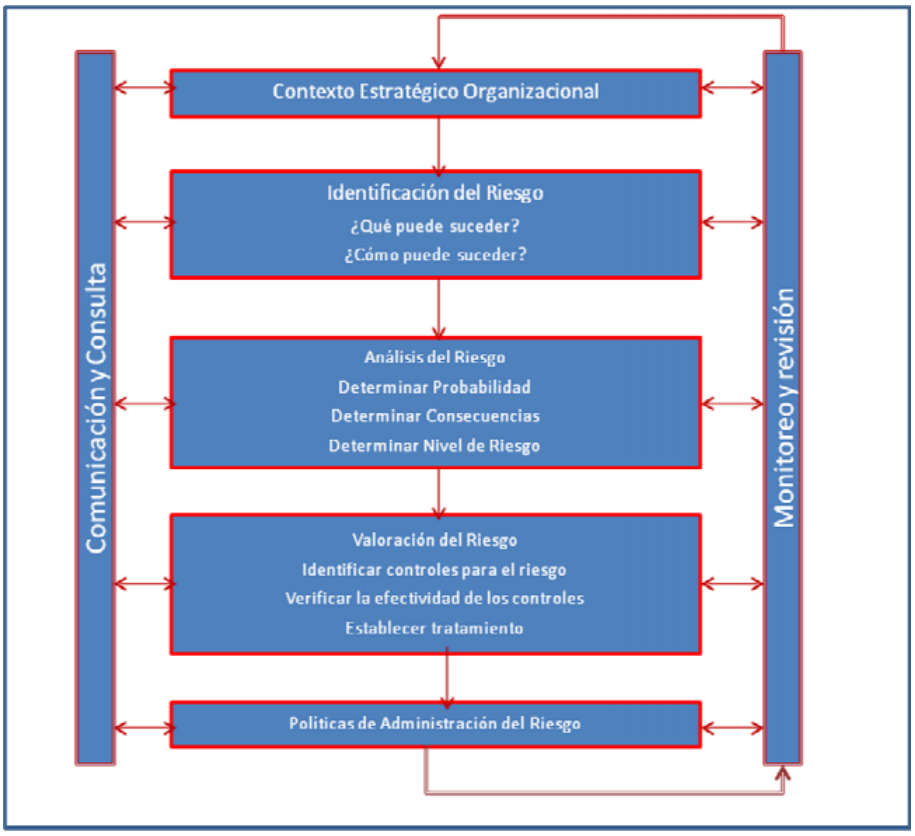

Imagen Tomada de la Cartilla de Administración de Riesgos del DAFP

DEFINICIONES

RIESGO: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

ADMINISTRACIÓN DEL RIESGO: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización. Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en

respuesta a un peligro determinado.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CAUSA: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros

AMENAZA: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución. (Materializar el riesgo).

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

PROBABILIDAD: Es la posibilidad que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

IMPACTO: Son las consecuencias que genera un riesgo una vez se materialice

CONTROL O MEDIDA: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

VALORACIÓN DEL RIESGO: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

PROCESO: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

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

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

CONTROL: Medida que modifica el riesgo.

POLITICA DE ADMINISTRACIÓN DE RIESGOS

El Instituto Municipal de Cultura de Yumbo se compromete a mantener una cultura de la gestión del riesgo asociado con la responsabilidad de diseñar, adoptar y promover políticas y planes regulando los riesgos de los procesos y proyectos, utilizando mecanismos y controles necesarios para la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y eficiencia a lo largo del ciclo de la vida para optimizar de manera continua y oportuna la respuesta a los riesgos de seguridad y privacidad de la información y seguridad digital de manera integral.

METODOLOGÍA

La gestión de riesgos de seguridad de la información deberá ser interactiva para las actividades de valoración de riesgos y/o tratamiento de estos.

ETAPAS

- Planear
- Establecer Contexto
- Valoración del Riesgo
- Planificación del Tratamiento del Riesgo
- Aceptación del Riesgo

IMPLEMENTAR

- Implementación del Plan de Tratamiento de Riesgo

GESTIONAR

- Monitoreo y Revisión Continuo de los Riesgos

MEJORA CONTINUA

- Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

En la siguiente imagen se visualiza la interactividad de las actividades para la valoración y tratamiento del riesgo en un proceso de la gestión del riesgo, estas actividades son: Establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo

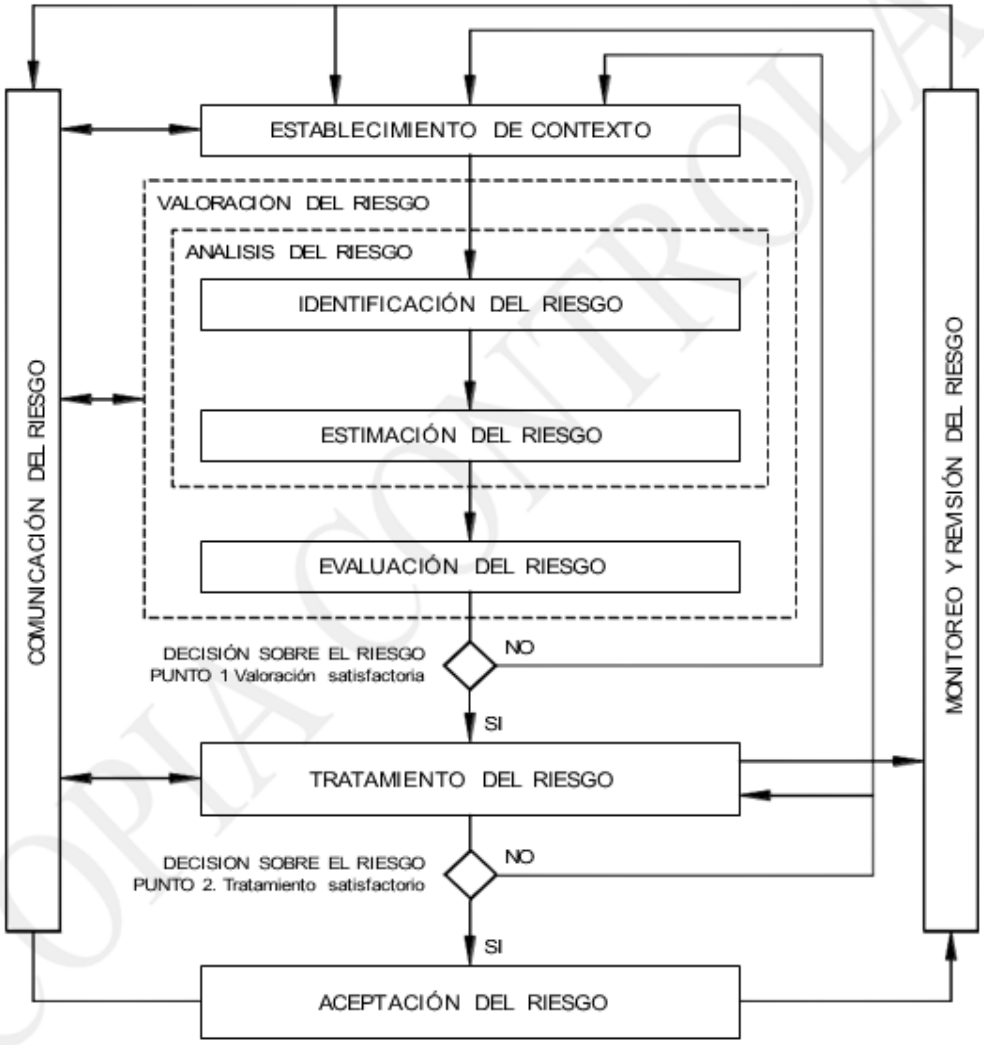

Imagen 1, tomada de: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), Norma Técnica Colombiana NTC-ISO/IEC 27005, 2009, página 6.

CONTEXTO ESTRATÉGICO

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte del IMCY y obtener los resultados esperados, basándose en la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos, así como la política de Seguridad de la Entidad. Esto debido a que es necesario tener claro el entorno o el contexto, qué procesos estarán involucrados, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

CRITERIOS BASICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

CRITERIOS DE EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Se desarrollarán criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos

- El valor estratégico del proceso de información en la Entidad
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación del IMCY.

CRITERIOS DE IMPACTO

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para el IMCY, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

CRITERIOS DE ACEPTACIÓN

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos del IMCY y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información.

IDENTIFICACIÓN DE RIESGOS

Para la evaluación de riesgos de seguridad de la información es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos.

Clasificación de activos:

1. Primarios:
    a. Procesos y actividades del Negocio
    b. Información
2. Soporte
    a. Hardware
    b. Software
    c. Redes
    d. Personal
    e. Sitio
    f. Estructura organizativa

ANÁLISIS DE RIESGOS

El IMCY documentara y especificara cada una de las etapas surtidas para el proceso de Gestión de Riesgos, así tener una guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria.

ESTIMACIÓN DEL RIESGO

Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**
- **Impacto**

PROBABILIDAD DEL RIESGO			
Concepto	**Nivel**	**Criterios de factibilidad**	Criterios de frecuencia
Raro	1	El evento puede ocurrir sólo en circunstancias Excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Pudo ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
Posible	3	Podría ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos 1 vez en el año
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla 2. Probabilidad del riesgo

IMPACTO DEL RIESGO			
Nivel	**Descriptor**	**Descripción**	**Criterios de frecuencia**
5	Insignificante	Si se presenta tendría consecuencias mínimas sobre la entidad	Más de una vez al año
10	Menor	Si se presenta tendría bajo impacto sobre la entidad	Al menos 1 vez en el año
15	Moderado	Si se presenta tendría mediana consecuencia sobre la entidad	Al menos 1 vez en los últimos 2 años
20	Mayor	Si se presenta tendría una alta consecuencia sobre la entidad	Al menos 1 vez en los últimos 5 años
25	Catastrófico	Si se presenta tendría desastrosa consecuencia sobre la entidad	No se ha presentado en los últimos 5 años

Tabla 3. Impacto del riesgo

EVALUACIÓN DEL RIESGO

Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

PROBABILIBAD	IMPACTO				
	Insignificante (5)	Menor (10)	Moderado (15)	Mayor (20)	Catastrófico (25)
Raro (1)	5	10	15	20	25
Improbable (2)	10	20	30	40	50
Posible (3)	15	30	45	60	75
Probable (4)	20	40	60	80	100
Casi Seguro (5)	25	50	75	100	125

Zona de riesgo baja: Asumir el riego
Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo
Zona de riesgo alta: Reducir el riesgo, evitar, compartir o trasferir
Zona de riesgo extremo: Reducir el riesgo, evitar, compartir o trasferir

Fuente: Guía de Riegos DAFP, adecuación Autor

TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

EVALUACIÓN

La evaluación del presente plan se realizara de acuerdo a las acciones establecidas dentro del mismo y con base en ellas se realizaran las mejoras necesarias para cumplir con el ciclo PHVA.