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

INSTITUTO MUNICIPAL

DE CULTURA DE YUMBO

IMCY 2020

OBJETIVO

identificar y analizar los Riesgos 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 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.

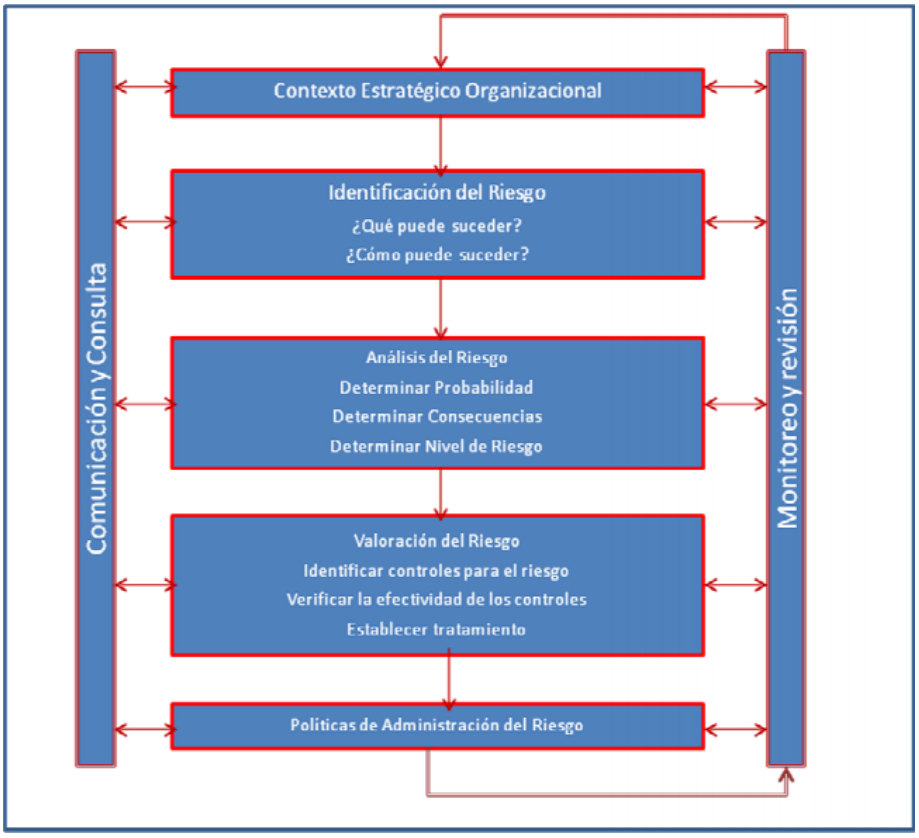

Imagen Tomada de la Cartilla de Administración de Riesgos del DAFP

La gestión de riesgos de seguridad de la información deberá ser iterativa 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.

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 en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, 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 o subprocesos y actividades del Negocio
    b. Información
    c. Actividades y procesos de negocio:
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		
Concepto	**Valor**	**Descripción**
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.
Improbable	2	Es muy poco factible que el evento se presente.
Posible	3	El evento podría ocurrir en algún momento.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias

IMPACTO		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	6	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Agencia. Tiene un impacto bajo en los procesos de otras áreas de la Agencia.
Moderado	7	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Agencia. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la ANI** y tiene un **impacto significativo en la imagen pública** de la Agencia y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	13	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Agencia**, tiene un **impacto catastrófico en la imagen pública de la Agencia y/o de la Nación**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

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:

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

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.