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

Alcaldía Distrital de Cartagena de Indias

TABLA DE CONTENIDO

CONTENIDO DE TABLAS

TABLAS DE FIGURAS

INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información se encuentra encaminado a desarrollar de manera eficiente y eficaz la gestión integral del riesgo logrando minimizar las posibles pérdidas, hurtos, alteraciones o cualquier manipulación indebida de los datos tratados en la alcaldía. Para un adecuado tratamiento de la información se encuentra la clasificación de los activos teniendo en cuenta la normatividad vigente de seguridad y privacidad de la información alineada con la NTC/IEC ISO 27000, la política de revelación de información, la política de tratamiento de datos personales, la política de seguridad y continuidad del servicio y al plan organizacional establecido, en cumplimiento los lineamientos generales de la política de Gobierno digital y las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores del MIPG.

4. OBJETIVO GENERAL

Diseñar e implementar el sistema de gestión de seguridad y privacidad de la información, con el fin de minimizar los riesgos a los cuales se expone la información, además de velar por el cumplimiento de los requerimientos legales, regulatorios y contractuales de la alcaldía

4.1. Objetivos específicos

- Determinar el alcance de la gestión integral del riesgo encaminados a la seguridad y privacidad de la información.
- Establecer las fases para la gestión integral del riesgo asociados a los procesos. Definir a través de una adecuada administración del riesgo, una base confiable para la toma de decisiones.
- Generar conciencia y cultura enfocada a la identificación de los riesgos de seguridad y privacidad de la información.

5. ALCANCE

La gestión de riesgos de seguridad y privacidad de la información junto con su tratamiento se aplicará a todas las dependencias de la Alcaldía Distrital de Cartagena de Indias, lo que incluye a todos sus funcionarios, contratistas, a toda la ciudadanía en general y a aquellas personas que por cumplimiento de los compromisos contractuales o en ejercicio de sus funciones realicen tratamiento de la información de la cual la alcaldía es responsable; así como a los diferentes activos de información que hacen parte del sistema de información.

Para lograr alcanzarlo es importante habilitar inicialmente las funciones de liderazgo para asesorar y apoyar el proceso de diseño, implementación y mantenimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información, seguido de una capacitación y generación de una cultura en la entidad para la gestión integral del riego.

6. NORMATIVIDAD

Tomando la metodología propuesta por la "Guía de Administración de Riesgos", Departamento Administrativo de la función Pública – DAFP se implementará la administración del riesgo en la Alcaldía Distrital de Cartagena de Indias con la finalidad de dar cumplimiento a la misión y visión Institucional y de la normatividad vigente que reglamentan la seguridad y privacidad de la información, por medio de la aplicación de buenas prácticas como COBIT5, ISO 27001:2013, ISO 27005, ISO 31000:2009.

7. ADMINISTRACIÓN DEL RIESGO

Para llevar a cabo una gestión integral del riesgo es importante entender cuáles son los activos de información, cómo se establece el sistema de información y reconocer los riesgos que se generarían sobre los mismos, las fallas, las vulnerabilidades, eventos o posibles incidentes de seguridad que se puedan llegar a presentar.
Las etapas por implementar son:

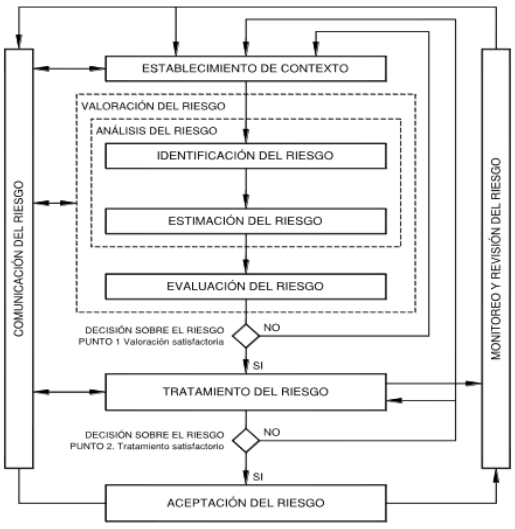

Figura No 1: Proceso de Gestión del Riesgo en la seguridad de la información
Fuente: Norma NTC ISO7/ IEC 27005 Por medio de estas etapas se desea apoyar

Por medio de estas etapas se desea apoyar al propietario del activo de información a identificar y clasificar los riesgos, así como el pilar la de información afectada, sus vulnerabilidades y amenazas.

Se establecen los siguientes tipos de riesgo:

- Fuga o pérdida de la información.
- Pérdida de confidencialidad por acceso no autorizado al activo de información que permite la utilización indebida o fraudulenta del mismo.
- Pérdida de integridad del activo de información que permite la utilización indebida o fraudulenta del mismo.
- Pérdida de disponibilidad del activo de información.
- Inadecuado tratamiento de los datos.

Los riesgos según su clasificación son:

Clasificación del riesgo	
1	**Riesgo Estratégico:** se enfoca en asuntos globales relacionados con la misión, la visión y el plan de desarrollo vigente, la clara definición de políticas, diseño y conceptualización de la entidad por parte del alcalde y su gabinete.
2	**Riesgo de Imagen:** están relacionados con la percepción y la confianza de las partes interesadas hacia la entidad.
3	**Riesgo Operativo:** comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y la articulación entre dependencias.
4	**Riesgo Financiero:** se relacionan con el manejo de los recursos de la entidad, que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
5	**Riesgo de Cumplimiento:** se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
6	**Riesgo de Infraestructura Física y Tecnológica:** están relacionados con la capacidad de infraestructura física y tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión, visión y el plan de desarrollo vigente.

Tabla No 1: Calcificación de riesgos

Fuente: Adaptación de la norma Técnica Colombiana NTC 5254

El análisis de riesgo permite determinar la severidad de este a partir del impacto y la probabilidad de su ocurrencia, así como también determinar el riesgo inherente de cada activo y asignar el responsable.

La probabilidad dirá cuál puede ser la ocurrencia del riesgo, pero sin tener en cuenta los controles con los que cuenta la administración para mitigar las vulnerabilidades. La escala para determinar el rango de la probabilidad inherente es:

Probabilidad			
Valor	**Nivel**	**Descripción**	**Frecuencia**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales y/o la eficacia de los controles es alta.	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento y/o la eficacia de los controles es moderada.	Al menos una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento y/o la eficacia de los controles es baja.	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias y/o la eficacia de los controles es nula.	Al menos una vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias y/o no existen controles o si existen es nula su eficacia.	Más de una vez al año

Tabla No 2: Escala de Probabilidad
Fuente: Adaptación de la norma Técnica Colombiana NTC 5254

Ahora bien, el impacto inherente en la Alcaldía Distrital de Cartagena de Indias, sin tener presente los controles al materializarse, debe verse en el peor de los escenarios posibles.

La escala de rangos para valorar los criterios de impacto en la entidad es:

Nivel de impacto						
Valor	**Nivel**	**Descripción**	**Confidencialidad de la Información**	**Imagen**	**Legal**	**Operativo**
1	**Insignificante**	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la alcaldía y/o la eficacia de los controles es alta	Personal	Grupo de Funcionarios	Multas	Ajustes a una actividad concreta
2	**Menor**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la alcaldía y/o la eficacia de los controles es moderada	Grupo de trabajo	Todos los Funcionarios	Demandas	Cambios en los procedimientos
3	**Moderado**	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la alcaldía y/o la eficacia de los controles es baja	Relativa al proceso	Usuarios ciudad	Investigación disciplinaria	Cambios en la interacción de los procesos
4	**Mayor**	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la alcaldía y/o la eficacia de los controles es nula.	Institucional	Usuarios Región	Investigación fiscal	Intermitencia en el servicio
5	**Crítico**	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la alcaldía y/o no existen controles o si existen es nula su eficacia.	Estratégica	Usuarios País	Intervención - Sanción	Paro total del proceso

Tabla No 3: Escala de Impacto

Fuente: Adaptación de la norma Técnica Colombiana NTC 5254

De la relación del impacto versus la probabilidad de ocurrencia se establece el nivel del riesgo, de la siguiente manera:

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Crítico (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

Tabla No 4: Administración del riesgo.

Fuente: Adaptación de https://swescom.wordpress.com/riesgo-y-administracion-del-riesgo/

Los riesgos identificados hay que tratarlos de acuerdo con la decisión que se realice en conjunto con la parte administrativa de la alcaldía, y saber qué manejo se le va a dar al riesgo, las opciones son:

Asumir	El riesgo se encuentra en un nivel que se puede aceptar sin necesidad de tomar otras medidas de control diferentes a las que se poseen.
Evitar	Se deben tomar las medidas encaminadas a prevenir su materialización.
Reducir	Se deben tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).
Transferir	Se debe involucrar a un tercero en su manejo, quien en algunas ocasiones puede absorber parte de las pérdidas ocasionadas por la ocurrencia.

Tabla No 5: C Definición de riesgos.

Fuente: adaptación definiciones de la Norma NTC ISO7/ IEC 27005

Una vez clasificados los riesgos se debe identificar e implementar controles como unas medidas que adopta la entidad para mitigar o anular la vulnerabilidad y reducir la probabilidad que se materialice el riesgo o reducir el impacto.

Los controles deben ser ejecutados bajo la responsabilidad de un encargado, describiendo las acciones de tratamiento, es decir los planes de mejora que deben tener su registro y seguimiento, algunos controles identificados están:

Controles de gestión	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento al cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos
Controles operativos	Conciliaciones
	Consecutivos
	Verificación de firmas
	Listado de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
Controles legales	Normas claras y aplicadas
	Control de términos

Tabla No 6: Ejemplos de Controles.
Fuente: adaptación definiciones de la Norma NTC ISO7/ IEC 27005

La valoración del riesgo, que es el resultado del producto de confrontar los resultados de la evaluación del riesgo con controles identificados, se hace con el fin de permitir establecer prioridades para el manejo y la asignación de políticas.

8. LINEAMIENTOS GENERALES

Los riesgos deben ser actualizados y construir nuevas acciones que permitan mitigarlos. El objetivo del enfoque de la administración de los riesgos es minimizar la calificación del riego, hasta llevarlo a un nivel bajo, por lo tanto, el riesgo que siga la zona de riesgo alta, extrema o moderada después de los controles se debe tratar con una acción correctica, y estas acciones registradas en el mapa de riesgos. Cuando se actualiza un riesgo se debe tener en cuenta la trazabilidad y la continuidad de las versiones anteriores, registrando las modificaciones y dejando evidencia de los cambios realizados para cada mapa de riesgos.

Es importante que los líderes de los diferentes procesos y subprocesos citen a mesas de trabajo cuando lo crean necesario, con el fin de generar espacios de participación de todos los servidores con el fin de minimizar la materialización de un riesgo y conseguir que los objetivos estratégicos.

9. GLOSARIO

- ✓ **Activo**: todo elemento que tenga valor en la entidad.
- ✓ **Análisis de riesgo**: se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- ✓ **Administración de riesgo**: etapas secuenciales que se deben desarrollar para un adecuado tratamiento de los riesgos.
- ✓ **Amenaza**: situación externa que no controla la entidad y que puede afectar su operación.
- ✓ **Análisis de Riesgo**: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis de riesgo inherente).
- ✓ **Causas**: elemento específico que origina el evento. Medias circunstancias y/o agentes que generan riesgo.
- ✓ **Clasificación del Riesgo**: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- ✓ **Consecuencia**: efectos que se pueden presentar cuando un riesgo se materializa.
- ✓ **Control**: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- ✓ **Frecuencia**: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- ✓ **Identificación del Riesgo**: etapa de la administración del riesgo donde se establece el riesgo con sus causas, consecuencias y se clasifica de acuerdo con los tipos de riesgos definidos.
- ✓ **Impacto**: medida para estimar cuantitativamente el posible efecto de la materialización del riesgo.

10. VIGENCIA Y CONTROL DE CAMBIOS

FECHA	AUTOR	VERSION	CAMBIOS
30 de enero 2020	Oficina Asesora de Informática	1.0	Versión inicial