ALCALDÍA MUNICIPAL DE CHÍA

OFICINA TIC

POLÍTICA ADMINISTRACIÓN DE RIESGOS

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Versión 1

CHÍA, MAYO 2019

CONTENIDO

INTRODUCCIÓN

La alcaldía municipal de Chía, dando cumplimiento al decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"[1] y la Guía para la administración del riesgo y el diseño de controles en entidades públicas del departamento de función pública. Establece los lineamientos para realizar la correcta administración de riesgos de seguridad de la información, identificación, clasificación, valoración, mitigación y tratamiento de los riesgos.

Teniendo en cuenta la norma técnica NTC-ISO/IEC 27001:2013, NTC-ISO/IEC 31000:2009 y NTC-ISO/IEC 27005; se debe realizar una gestión de riesgos de seguridad de la información, donde se identifiquen los activos con su respectivo criterio de impacto, valoración de amenazas y vulnerables.

[1] Tomado del decreto número 1008 de 2018

1. OBJETIVO

Establecer la política para la identificación, clasificación y valoración de los riesgos digitales o de seguridad de la información en la alcaldía municipal de Chía, basado en la política de gobierno digital y la guía de administración de riesgos del Departamento Administrativo de la Función Pública – DAFP.

2. ALCANCE

Aplica a todos los procesos, secretarías y dependencias de la alcaldía municipal de Chía, desde la matriz de inventario de activos de información hasta el plan de tratamiento de riesgos.

3. GLOSARIO

- **Activo:** cualquier cosa que tiene valor para la organización[2], es decir, todo elemento que contenga información (hardware, información, software, servicios y recurso humano) y cuyo valor garantice el correcto funcionamiento de la entidad o dependencia.

- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.[3]

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera[4].

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.[5]

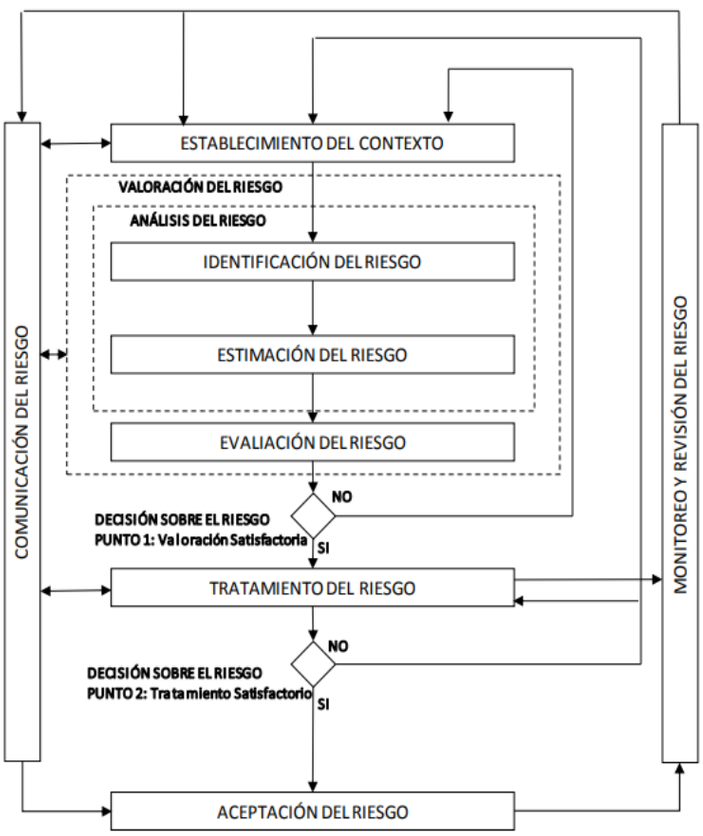
[2] (ICONTEC, 2013)
[3] (ICONTEC, NTC ISO/IEC 27000:2013, 2013)
[4] (ICONTEC, NORMA TÉCNICA NTC-ISO/IEC 27001, 2013)
[5] (ICONTEC, NORMA TÉCNICA NTC-ISO/IEC 27001, 2013)

4. POLÍTICA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La política de administración de riesgos de seguridad de la información, tiene como objetivo establecer los parámetros para la correcta administración y tratamiento de los riesgos que pueda tener la alcaldía municipal de Chía en sus diferentes procesos

La metodología que utiliza la alcaldía municipal de Chía para la adecuada administración de riesgo de seguridad de la información es la norma NTC-ISO/IEC 27005 (véase figura 1).

Figura 1 Administración del riesgo



Fuente: NTC-ISO/IEC 27005[6]

[6] Norma NTC-ISO/ IEC 2005

4.1. Establecimiento del contexto

El contexto estratégico de la administración de riesgos, se debe establecer con los objetivos de los procesos, las partes interesadas, la estructura de la alcaldía municipal de Chía, el alcance y el límite que va a tener el tratamiento de riesgos.

4.2. Identificación del riesgo

La identificación de los riesgos tiene como objetivo establecer las posibles amenazas y vulnerabilidades que lleve a una pérdida de información o económica en los activos de información de la alcaldía municipal de Chía.

4.2.1. Identificación de los activos de información

La identificación de los activos de información se realiza en cada proceso de la entidad, teniendo en cuenta la guía para el inventario, valoración y clasificación de los activos de información de la alcaldía municipal de Chía, donde se establece el nombre del activo, la descripción del activo, tipo de activo, ubicación, atributos, propiedad y clasificación de la información.

4.2.2. Identificación de las amenazas:

Amenazas que pueden afectar un activo, teniendo en cuenta que las amenazas tienen como objetivo causar daño a un activo a partir de una vulnerabilidad detectada en uno o varios activos de información causando impactos en los diferentes procesos de la entidad, las amenazas se clasifican de la siguiente manera (véase cuadro 4):

Cuadro 1 Amenazas

TIPO	AMENAZA
Daños ambientales	Inundación.
	Incendio.
Acciones no autorizadas	Ataques a los equipos de cómputo.
	Divulgación de información.
	Acceso no autorizado a la información.
	Virus informático.
	Phishing (Abrir correos o archivos desconocidos).

	Programas espías.
Compromiso de los funcionarios	Empleados disgustados.
Pérdida de los servicios esenciales	Pérdida de suministro de energía.
	Falla en el aire acondicionado.
Compromiso de la información	Hurto de equipos.
	Espionaje.
	Robo de información.
	Ataques de fuerza bruta.

4.2.3. Identificación de los controles existentes

Tiene como objetivo establecer el estado actual de los controles de la norma ISO 27001 en su versión más reciente, para evitar duplicidad de controles e identificar que controles se están cumpliendo y cuales son necesarios para realizar el plan de tratamiento de riesgos.

4.2.4. Identificación de la vulnerabilidad

Vulnerabilidad que puede ser explotada por una amenaza y pueda afectar un determinado activo de información.

4.2.5. Probabilidad

La probabilidad se determina por el número de veces que pueda ocurrir o presentarse el riesgo.

Cuadro 2 Probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA		
Valor	Concepto	Frecuencia
5	Casi certeza	Puede ocurrir semanalmente.

4	Probable	Probable que ocurra mensualmente.
3	Posible	Puede ocurrir semestralmente.
2	Improbable	Puede ocurrir anualmente.
1	Raro	Puede ocurrir cada cuatro años.

4.2.6. Impacto:

El impacto se clasifica de la siguiente manera teniendo en cuenta las consecuencias financieras que se pueden generar en la entidad (véase cuadro 6):

Cuadro 2 Impacto

IMPACTO		
Valor	Nivel de impacto	Impacto financiero
5	Catastrófico	Mayor a $1.000.000.000
4	Mayor	Entre $100.000.000 a $1.000.000.000
3	Moderado	Entre $10.000.000 a $100.000.000
2	Menor	Entre $1.000.000 a $10.000.000
1	Insignificante	Menor a $1.000.000

4.2.7. Nivel de riesgo:

El nivel de riesgo se calcula mediante la multiplicación del valor de la probabilidad de ocurrencia y el impacto que puede ocasionar el riesgo en el activo de información.

4.3. Evaluación del riesgo

La evaluación de riesgos se basa en clasificar los riesgos de cada proceso de la alcaldía municipal de Chía, de acuerdo a la calificación de la probabilidad e impacto de la identificación de riesgos, tipo de impacto basado en la confidencialidad, integridad y disponibilidad, zona de riesgo dependiendo del mapa de calor donde se realiza la ubicación de los riesgos, teniendo en cuenta la calificación y la medida de respuesta para reducir, evitar, compartir o transferir el riesgo.

4.4. Tratamiento de riesgo

El plan de tratamiento de riesgos se realiza para reducir, mitigar, evitar, compartir o transferir los riesgos encontrados en la evaluación de los riesgos, estableciendo los tipos de controles que se pueden implementar para mitigar la probabilidad o impacto, puntaje al ejercer el control, seguimiento al control, nueva calificación dependiendo del control a implementar, acciones para implementar el control, responsable de realizar las acciones al riesgo e indicadores para realizar la medición de los controles y la reducción del riesgo.

La declaración de aplicabilidad se realiza para identificar los controles que se van a utilizar para el plan de tratamiento de riesgos, de acuerdo a la norma ISO 27001 en su versión más reciente Anexo A, un listado de los dominios (14), objetivos de control (35) y controles (114); y debe ser aprobado por la alta dirección.

4.5. Aceptación del riesgo

De acuerdo al plan de tratamiento de riesgos y los controles que se van a implementar para reducir la probabilidad e impacto de un riesgo, la alta dirección y el jefe o dueño del proceso donde se encuentra el riesgo, determina si acepta las acciones para el tratamiento de riesgos.

4.6. Evaluación y monitoreo

De acuerdo a los indicadores establecidos en el tratamiento de riesgo, se verifica de acuerdo al tiempo determinado del indicador, para verificar que el tratamiento de riesgo se esté cumpliendo.

4.7. Actualización administración de riesgos

La administración de riesgos se debe actualizar cada año, verificando los indicadores de los controles y las acciones de los riesgos encontrados en el anterior plan de tratamiento de riesgos.

ACTA DE REUNIÓN

ALCALDÍA MUNICIPAL DE CHÍA	ADIMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN		
	ACTA DE REUNION	CÓDIGO	ASIG-FT01-V1
		PAGINAS	1 de 2

PROCESO:

DEPENDENCIA: Oficina TIC

RESPONSABLE DE LA REUNIÓN: Jonathan Sebastian Gomez Diaz

OBJETIVO:

☐ Consejo. _____
☐ Comité. _____
☒ Reunión: Análisis y aprobación política de administración de riesgos de seguridad informática.

ACTA N°	1	FECHA	30 - 05 - 2019
LUGAR	Oficina TIC		

ASISTENTES	NOMBRE	NÚMERO DE IDENTIFICACIÓN	CARGO/ DEPENDENCIA	CORREO ELECTRÓNICO
	Jorge Iván Ortiz A.	11203134	Jefe Oficina TIC	oficinatic@chia.gov.co
	Vivian Andrea C.	39199807	Prof. Universitario	vivian.chacon@chia.gov.co
	Jonathan Sebastian G.	1072355094	Contratista	jonathan.gomez@chia.gov.co
	Ingrith Katherinne G.	1077702256	Contratista	katherinne.quintero@chia.gov.co

ORDEN DEL DÍA

1. Registro y Asistencia
2. Lectura y aprobación del orden del día.
3. Lectura y análisis de la "Política de administración de riesgos de Seguridad Informática".
4. Aprobación o desarrollo de observaciones de la política.
5. Definir compromisos y responsables.
6. Firmar acta.

DESARROLLO DEL ORDEN DEL DIA

1. Se inicia la reunión haciendo el llamado a los asistentes y se organiza el grupo de trabajo.
2. Se procede a leer el orden del día y se inicia la mesa de trabajo con todos los presentes.
3. El jefe de la Oficina TIC Jorge Iván Ortiz procede a leer la política de administración de riesgos de seguridad elaborada por la Ing. Katherinne Quintero y junto con la supervisora Andrea Chacón analizan los aspectos técnicos del documento.
4. Se da por aprobada la "Política de administración de riesgos de seguridad informática".

ALCALDIA MUNICIPAL DE CHIA	ADIMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN		
	ACTA DE REUNION	CÓDIGO	ASIG-FT01-V1
		PAGINAS	2 de 2

5. Se define un compromiso: enviar oficio al comité del MIPG para inclusión de la política de administración de riesgos de seguridad informática en el MIPG con la guía de administración de riesgos.
6. Se firma el acta y se da por terminada la reunión.

ANEXOS

- Política de administración de riesgos de seguridad informática.

FIRMAS

Jefe Oficina TIC

Ingrith K. Quintero
Contratista Oficina TIC

Jonathan Gómez
Contratista Oficina TIC

COMPROMISOS

ACTIVIDAD	RESPONSABLE	FECHA
- Redactar oficio al comité de MIPG para inclusión de política.	- Jonathan Sebastian Gómez Diaz.	31/05/2019

OFICIO OTIC-037-2019

ALCALDÍA MUNICIPAL DE CHÍA
1003

OFICINA TIC

OTIC – 037 - 2019

Chía, 31 de Mayo de 2019

Señores.
SECRETARÍA GENERAL
SECRETARÍA DE PLANEACIÓN
COMITÉ MUNICIPAL DE GESTIÓN Y DESEMPEÑO - MIPG
Chía Cundinamarca.

Cordial Saludo

La Oficina de Tecnologías de la Información y las Comunicaciones en pro del desarrollo de las diferentes actividades que forman parte de la Política de Gobierno Digital, se ha registrado a la Administración Municipal en el concurso denominado "Máxima Velocidad", una iniciativa del MinTIC que busca promover la transformación digital del Estado cumpliendo diferentes retos propuestos para las entidades inscritas en el mismo.

Por lo anterior, el concurso en una de sus categorías (Metodología de Gestión de Riesgos de Seguridad Digital), solicita que la Alcaldía Municipal de Chía dentro de su Modelo Integrado de Planeación y Gestión adopte una política de riesgos de seguridad digital. Esta política ya está redactada, revisada y aprobada por la Oficina TIC y se adjunta a este oficio junto con el acta de reunión escaneada con el objetivo de analizar y aprobar la política de administración de riesgos de seguridad informática.

Agradezco de antemano la colaboración prestada y quedo atento a su respuesta en el menor tiempo posible.

JORGE IVAN ORTIZ ARDILA
Jefe Oficina TIC
Alcaldía Municipal de Chía
Elaboró: Sebastián Gómez - Contratista
Revisó: Andrea Chacón – Profesional Universitario

Cra 11 # 11 - 29 PBX: 884 44 44 Ext. 2300 - 2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co
Sí... Marcamos la DIFERENCIA