POLITICA DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Dimensión MIPG: Gestión con valores para el resultado.

Alcaldía Municipal De Quibdó

2019

Carrera Segunda No 24A - 32, Telefax 671 21 75 Código Postal: 270001.
Correo-e: alcaldia@quibdo-choco.gov.co. Quibdó - Chocó.

1. OBJETIVO

Establecer y formalizar de forma general el tratamiento de riesgos de seguridad de la información, en la alcaldía Municipal de Quibdó.

2. ALCANCE

El documento incluye la matriz de riesgos para el tratamiento de los riesgos y necesidades de la seguridad de la información, en todos los procesos de la Alcaldía Municipal de Quibdó.

3. MARCO NORMATIVO

- La Ley 1712 de 2014. "Ley de transparencia y del derecho de acceso a la información pública nacional". ¬
- La Ley 1581 de 2012 y decreto 1377 de 2013. "Ley de protección de datos personales". ¬
- La Ley 1273 de 2009. "Ley de delitos informáticos y la protección de la información y de los datos". ¬
- Decreto 1078 del 26 de mayo de 2015. Por medio del cual se expide el "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". ¬
- La Ley 527/1999. "Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones". ¬
- Decreto 612 del 4 de abril de 2018, "por el cual se fijan directrices para la integración de planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado". ¬
- Decreto 1008 del 14 de junio de 2018, "Por el cual se establecen los lineamientos generales de la política Gobierno Digital".

DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas**: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos**: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del 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 del riesgo inherente).
- **Asumir el riesgo**: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa. • Causa: medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo**: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo**: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia**: efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico**: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control**: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo**: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Matriz de Tratamiento de Riesgos de seguridad y privacidad de la información

Área / Macroproceso	Proceso	Riesgo	Tratamiento del Riesgo	Tipo de Riesgo	Probabilidad	Impacto
SECRETARIA GENERAL	SISTEMAS	Ausencia de un análisis de riesgo, frente al riesgo actual y el riesgo aceptado para la perdida de información	Conocer los efectos legales de la materialización de los riesgos asociados a la seguridad de la información	Operativo	2	3
		Debilidades en los procesos de control de cambios	Establecer que las claves de acceso deben ser modificadas de maneras obligatoria, periódicamente	Tecnológico	3	3
		Debilidad en las configuraciones de seguridad tanto de software como hardware	Realizar evaluaciones de ciberseguridad en los equipos como en las redes	Operativo	1	2
		Dispositivos y aplicaciones conectados a la red sin autorización	Limitar el acceso a dispositivos externos, requiriendo para su uso autenticación	Operativo	4	1
		Permisos no autorizados para borrar, crear y eliminar datos	Contar con protección en antivirus y filtración de sitios web maliciosos actualizados	Tecnológico	4	1
		Ausencia de una matriz de clasificación de la información de acuerdo al riesgo que representa	Incluir dentro del mapa de riesgos, los riesgos asociados a compartir información entre funcionarios y terceros. D22	Estratégico	4	0
		Ausencia de un inventario de la información clasificada	Realizar periódicamente un inventario de la información que se administra según su ubicación, clasificación y ubicación	Operativo	3	1
		Ausencia de una política de eliminación y retención de la información	Construir política para el almacenamiento, custodia y destrucción de la información	Estratégico	4	1
		Falta de actualización de las políticas de seguridad de la información	Actualizar de acuerdo a los cambios en la información de lipolitica de seguridad de la información	Estratégico	3	2
		Debilidades en el procedimiento para la realización de las copias de seguridad	Definir la metodología y los medios para el desarrollo de copias de seguridad	Operativo	3	3
		Permitir que se pueda extraer información de los equipos por dispositivos externos (USB)	Evaluar la aplicación de controles, de tal forma que los mismos sean actualizados de acuerdo con los riesgos emergentes	Operativo	4	1
		Limitaciones en el acceso remoto a los equipos y dispositivos móviles en caso de pérdida o robo para ser bloqueados y no permitir el acceso a la información	Los accesos remotos se realizarán por medio de VPN, así como requerir la autenticación de los usuarios con dos registros de confirmación	Tecnológico	4	1
		Limitada formación a los funcionarios en controles de seguridad para la administración de la información	Realizar un plan de formación y entrenamiento en ciberseguridad	Estratégico	3	1
		Desconocimiento de los colaboradores para saber cómo deben actuar frente a un posible ataque externo a la información.	Formar en cada cargo frente a la responsabilidad en ciberseguridad y sus consecuencias laborales/o sanciones, frente al incumplimiento de las acciones que se deben desarrollar desde la perspectiva de ciberseguridad	Operativo	3	1

RESPONSABLE DEL DOCUMENTO
Jefe Área de Tecnologías y Sistemas de Información

Otras disposiciones

- Cualquier modificación de la presente política, será aprobada por el Alcalde.
- Las aclaraciones de interpretación sobre la presente política serán resueltas por la Oficina de Sistemas
- Entra en vigor la presente política a partir del 31 de enero de 2019.
- El documento original de la presente política se encuentra suscrito por: el alcalde Municipal de Quibdó

ISAIAS CHALA IBARGUEN
Alcalde Municipal

Elaboró	Revisó	Aprobó	Suscribe
Mónica B. Murillo Contratista	**Yonatan Copete Rúgeles** Jefe Oficina de Sistemas	**Julio Á[illegible]** Secretario técnico Comité gestión y Desempeño Institucional	**Isaias Chala Ibarguen** Alcalde Municipal