Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Quibdó 2024-2027

Proyectó:

Aprobó:

Visto Bueno:

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

Introducción

Actualmente en Colombia y cada una de sus regiones se viene implementando la Política de Gobierno Digital, como indica el decreto 1008 de 14 de junio del 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".

La Política de Gobierno Digital cuenta con un nuevo enfoque en donde no sólo el estado sino también los diferentes actores de la sociedad, son actores fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público. De igual forma, cuenta con líneas de acción que orientan el desarrollo y la implementación de la política, dos componentes TIC para el Estado y TIC para la Sociedad y tres habilitadores transversales Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se basa en una orientación de estrategias preventivas, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, adicionalmente se busca desarrollar mecanismos para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con alta objetividad, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia establece que la seguridad de la información es un elemento que apoya a las entidades de manera trasversal, habilitando el desarrollo de los componentes de la

política de Gobierno Digital, desarrollado a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones entre sus propósitos pretende lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información, que consiste en desarrollar procesos y procedimientos que hagan uso de las tecnologías de la información, a través de la incorporación de esquemas de manejo seguro de la información y de la alineación con la arquitectura institucional de la entidad (Arquitectura misional y Arquitectura de TI), a fin de apoyar el logro de las metas y objetivos de la entidad. En ese sentido, teniendo en cuenta el nuevo concepto de Gobierno Digital y la alineación de la Política de Gobierno Digital, acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, Controles de Seguridad y Privacidad de la Información, se estipulan los lineamientos del presente plan.

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

Objetivo General

Establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como un instrumento que permita adoptar medidas y acciones encaminadas a controlar y minimizar los riesgos de seguridad y privacidad de la información de la Alcaldía de Quibdó.

Alcance

Todos los lineamientos establecidos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información están orientados a gestionar los riesgos de los servicios de tecnologías de información y comunicaciones, y son aplicables a cada uno de los procesos estratégicos, misionales y de apoyo de la administración municipal, por lo cual deberán ser cumplidos por toda la entidad, sus funcionarios, contratistas y terceros de la Alcaldía de Quibdó y la comunidad en general.

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

Marco Teórico

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 lineamientos generales de la política Gobierno Digital”.

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

Proceso Para El Tratamiento De Riesgos De Seguridad Y Privacidad De La Información

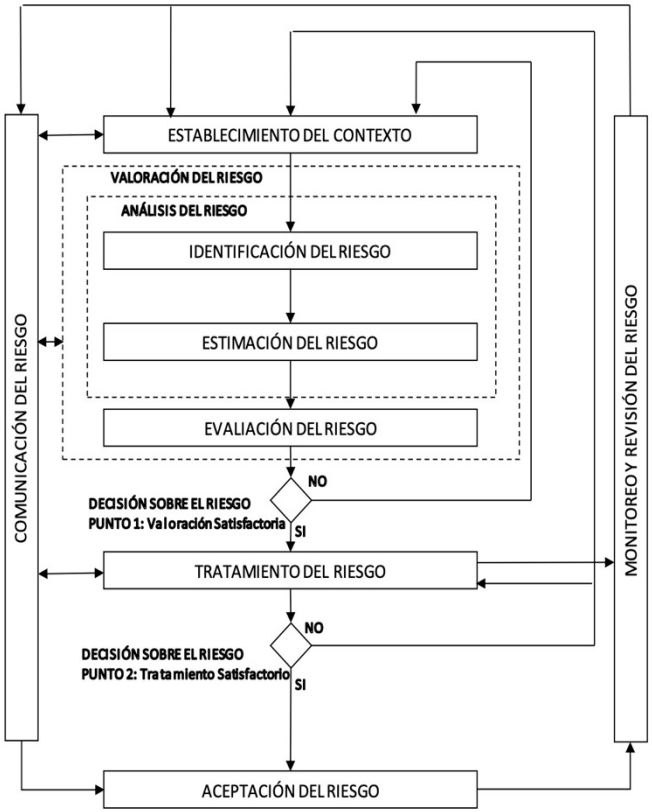
La gestión del riesgo es aplicada a cada uno de los procesos estratégico, misional y de apoyo de la entidad. Para el tratamiento de riesgos de seguridad y privacidad de la información se tomará como insumo los activos del Modelo de Seguridad y privacidad de la Información – MSPI, sobre la cual se implementará el presente Plan.

CRITERIOS DE CLASIFICACIÓN		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

NIVELES DE CLASIFICACIÓN	
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf



Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

Matriz de Tratamiento de Riesgos de seguridad y privacidad de la información				
Área/ Macro proceso	**Proceso**	**Riesgo**	**Tratamiento del Riesgo**	**Tipo de Riesgo**
OFICINA DE SISTEMAS	**SISTEMAS**	Ausencia de un análisis de riesgo, frente al riesgo actual y el riesgo acoplado para la pérdida de información	Conocer los efectos legales de la materialización de los riesgos asociados a la seguridad de la información	Operativo
		Debilidades en los procesos de control de cambios	Establecer que las claves de acceso deben ser modificadas de manera obligatoria, periódicamente	Tecnológico
		Debilidad en las configuraciones de seguridad tanto de software como hardware	Realizar evaluaciones de ciberseguridad en los equipos como en las redes	Operativo
		Dispositivos y aplicaciones conectados a la red sin autorización	Limitar el acceso a dispositivos externos, requiriendo para su uso autenticación	Operativo
		Permisos no autorizados para borrar, crear y eliminar datos	Contar con protección en antivirus y filtrado de sitios web maliciosos actualizados	Tecnológico
		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 informaciónentre funcionarios y terceros.	Estratégico

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

		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
		Ausencia de una política para el tratamiento de riesgos de seguridad y privacidad de la información	Construir política para el tratamiento de riesgos de seguridad y privacidad de la información	Estratégico
		Falta de actualización de las políticas de seguridad de la información	Actualizar de acuerdo a los cambios en la información de seguridad de la información	Estratégico
		Debilidades en el procedimiento para la realización de tas copias de seguridad	Definir la metodología y los medios para el desarrollo de copias de seguridad	Operativo
		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
		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

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001

		Limitada formación a los funcionarios en controles de segundad para la administración de la información	Realizar un plan de formación y entrenamiento en ciberseguridad	Estratégico
		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

Tel: (4) 6712175
contacto@quibdo-choco.gov.co
www.quibdo-choco.gov.co
Carrera 2 #24a-32 / Quibdó-Chocó
Código postal 270001