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

INTRODUCCIÓN

Con la finalidad de actualizar el Plan de tratamiento de Riesgos donde se establezcan medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de la Personería Distrital de Buenaventura, empleando los cuadros de referencia como la ISO27005:2011, ISO27001 y los estándares que nos ayudan a mitigar los riesgos acogiendo mejores habilidades en la ejecución de los procesos.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión

1. OBJETIVOS

Objetivo General

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de

Objetivos Específicos

- Encontrar puntos priorizados en cada activo de la información por medio del inventario de la entidad.
- Establecer las políticas de seguridad en la información, salvaguardando la confiabilidad integral en la disponibilidad de la información.

2. ALCANCE

Este documento tiene como fin mejorar el análisis, la evaluación y el control de los riesgos de seguridad, que se ocasionan por las actividades diarias y el uso de la información institucional en la Personería Distrital de Buenaventura.

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

El esquema de este documento se cimenta de acuerdo a los lineamientos planteados por el Ministerio de las TIC y los estándares ISO 27001:2013, ISO 31000:2018, para establecer los principios e implementar un sistema de gestión de riesgos, cuyo objetivo es minimizar, gestionar y controlar cualquier tipo de riesgo teniendo en cuenta el origen, la causa y su grado de incidencia.

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

Personería Distrital de Buenaventura llevó a cabo la expansión adecuada de diversas figuras importantes en el tema de plan de tratamiento del riesgo de la privacidad y seguridad de la información, ya que a través de ellos se pudo dar definición de algunas concepciones que se consideran de gran relevancia para mitigar los riesgos identificados en la entidad, este mismo busca ejecutar un proceso de gestión de los riesgos, adoptando medidas y acciones encaminadas a minimizar los mismos, preservando la confidencialidad, integridad y disponibilidad de la información. Este asunto confiere en instaurar un estudio de caracterización de riesgos de forma preventiva para proceder a realizar un tratamiento y administración de estos.

4. DEFINICIONES

Análisis de riesgo: es el uso sistemático de la información disponible para determinar la frecuencia con la que determinados eventos se pueden producir y la magnitud de sus consecuencias.

Activo: Es un recurso que tiene un valor específico para la entidad y debe ser protegido.

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.

Acciones asociadas: Son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo.

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.

Causa: Medios, circunstancias y/o agentes que generan riesgos.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Evento de seguridad: Situación previamente desconocida que puede ser relevante para la seguridad.

Mapa de riesgos: Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: Ocurrencia del riesgo identificado.

Riesgo: Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

5. ROLES Y RESPONSABILIDADES

Es fundamental distinguir con claridad los objetivos institucionales y estratégicos de la Personería Distrital de Buenaventura, adentrarse en una mira sistémica de la gestión, de manera que se analicen las oportunidades o amenazas notables que puedan crear riesgos e inquieten el cumplimiento de los objetivos misionales de la entidad.

Sistemas de Información: La construcción del Plan de Tratamiento de Riesgos es responsabilidad del proceso Sistemas de Información. La administración de los riesgos de

seguridad y privacidad depende de la participación de todo el equipo de funcionarios y contratistas de la Personería Distrital de Buenaventura.

Oficina Asesora de Planeación: Se encarga de evaluar, aprobar las directrices para la administración del riesgo y ejecución de controles, con el objetivo de minimizar los riesgos que afecten las gestiones de los procesos y la entidad.

Líderes de los Procesos: Responsables de identificar los riesgos y crear acciones para menguarlos, determinando los modos y causas, al igual que la ostentando evidencias para el plan de mejoramiento de los procesos.

6. POLITICAS DE GESTIÓN DEL RIESGO

- Implementar la Política de Seguridad y Privacidad de la información.
- Seguridad de la Información enfocada a los recursos humanos.
- Revisión de los Controles de acceso.
- Gestión de incidentes de Seguridad de la Información.

Para menguar los riesgos, es fundamental que se destinen recursos humanos, tecnológicos, operativos y de presupuesto que permitan de una manera continua ejecutar esbozos de trabajo y acciones para mejorar las políticas de seguridad y privacidad existentes.

7. RIESGO

Definición

Es la posibilidad de sufrir daños o pérdidas. La amenaza es un componente del riesgo y se puede considerar como: un agente de amenazas ya sea voluntario o involuntario, como identificar y explotar una vulnerabilidad, que ofrece un resultado inesperado y no deseado

8. CARACTERIZACIÓN DEL RIESGO

La caracterización del riesgo consiente en conocer las ocurrencias que puedan surgir frente a las alteraciones en el funcionamiento de la entidad, y pueden complicar y afectar la confidencialidad, integridad y disponibilidad de la información.

El propósito fundamental de caracterizar el riesgo es determinar que puede ocurrir en el caso de tener una perdida potencial de información y que acciones tomar al comprender la causa y el dónde y por qué puede ocurrir el evento.

Riesgos	Causas
Daño en los equipos tecnológicos.	- Falta de mantenimiento. - Uso inadecuado de las herramientas tecnológicas
Pérdida de la conexión.	- Daños en el proveedor
Correos electrónicos no seguros.	- Desconocimiento de los riesgos al acceder a correos falsos. - Instalación de programas espías. - Fallas en los filtros de seguridad o mala configuración del servidor.
Pérdida, Hurto o Evasión de Información.	• Fallas en el proceso del respaldo de la información o restauración de la misma. • Fallas en los análisis y socialización de las

9. INDIVIDUALIZACIÓN DE LAS AMENAZAS

Las amenazas ocasionan daños a los activos como información, procesos y sistemas lo que produce el detrimento a cualquier entidad. Estas amenazas pueden ser fortuitas o voluntarias, por lo que pueden ser accidentales o deliberadas. Estas amenazas se deberían distinguir genéricamente.

TIPO	AMENAZA
Eventos naturales	Fenómenos Climáticos, polvo, corrosión
Daño físico	Pérdida del suministro de energía
Acciones no autorizadas	Uso no autorizado del equipo
	Corrupción de datos
	Procesamiento ilegal de datos
	Acceso forzado al sistema
Pérdida de los servicios esenciales	
	Falla en equipos de comunicaciones
	Fallos en discos de datos
Compromiso de la información	Hurto de documentos
	Robo de equipos de computo
Fallas técnicas	Fallas en equipos
	Fallas en el diseño de software
	Faltas de mantenimiento
Acciones no autorizadas	Uso no autorizado de equipos
	Copias ilegales de software y datos reservados

10. TRATAMIENTO DEL RIESGO

El Tratamiento del Riesgo de la Personería Distrital de Buenaventura debe distinguir las siguientes opciones para tratar los riesgos:

Evadir el riesgo

• Esta opción de tratamiento busca eliminar la probabilidad de ocurrencia o el impacto del riesgo, tomar las medidas necesarias para prevenir la materialización del riesgo.

Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

Comprimir riesgos • Se efectúa cuando el riesgo se puede tratar internamente y puede llevarse a un nivel aceptable.

Asumir el riesgo • Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el jefe del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.