PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACIÓN 2024

ALCALDIA MUNICIPAL DE PLATO MAGDALENA

Armando Campuzano Restrepo

Alcalde Municipal 2024 - 2027

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACIÓN 2024

ALCALDIA MUNICIPAL DE PLATO MAGDALENA

Armando Campuzano Restrepo

Alcalde Municipal 2024-2027

"La vía nos une"

DEPARTAMENTO ADMINISTRATIVO DE PLANEACION MUNICIPAL
ÁREA DE SISTEMAS

Plato Magdalena

2024

INTRODUCCIÓN

En el país en la actualidad se adelanta la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información (MSPI). No obstante, el manual está amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular al principio de Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de

riesgos preservando confidencialidad, integridad y disponibilidad de la información de las entidades del estado, y de los servicios que prestan al ciudadano. Es por ello que es parte fundamental en el cumplimiento de los objetivos de una organización, en este caso para la Administración del Municipio de Plato, Magdalena, debe salvaguardar todo tipo de información ya que podría presentarse alteración, mal uso, pérdida entre otros muchos eventos. En este orden de ideas, detectar a tiempo los posibles riesgos de perdida, es una estrategia metodológica y sistemática que garantizará el buen uso que se da a la información.

El propósito de un Sistema de Gestión de la Seguridad de la Información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La importancia de que las administraciones estatales cuenten con un Plan de Tratamiento de Riesgos de Seguridad de la información, este aporta la evidencia de los niveles de riesgos en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a los funcionarios a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recurso.

La adopción e implementación del Modelo de Seguridad y Privacidad de la información en las entidades públicas toma como sustento el estándar NTC ISO 27001:2013, así como principios regulatorios definidos por el Gobierno Nacional, tal como la Ley 1712 de 2014 o la Ley 1581 de 2012; así mismo, apoyan su enfoque en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información, para lo cual se ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción y de seguridad de la información.

La adopción de prácticas de gestión de riesgos en las entidades públicas permitirá fortalecer la toma de decisiones en cuanto a la implementación de controles de acuerdo con el plan de tratamientos definido.

Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información con enfoque en la seguridad informática frente a ciber amenazas sobre activos de tecnologías de información y de las comunicaciones del Centro de Datos Corporativo.

1. OBJETIVOS

1.1. Objetivo General

Implementar, establecer y gestionar un plan de acción que permita controlar y aportar al tratamiento de riesgo de seguridad y privacidad de la información, que soportan la prestación de servicios digitales de la Entidad, desde el enfoque de la seguridad informática frente a ciber amenazas, así mismo minimizar los riesgos de seguridad y privacidad de la información, relacionados a los procesos TIC existentes en el Municipio de Plato Magdalena, de esta manera fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

1.2. Objetivos Específicos

- Concientizar a todos funcionarios, contratistas y terceros en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.

- Aplicar las metodologías del DAFP e ISO, respectivamente, en seguridad y riesgo de la información, para la Administración Central Municipal de Plato.

- Hacer partícipes y responsables a los funcionarios de la entidad de la magnitud y relevancia de mantener información confiable.

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

2. ALCANCE

Este Plan se enfocará en fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el departamento administrativo de la función pública, enfocados a la seguridad informática, teniendo en cuenta las capacidades y recursos disponibles para todos los empleados, funcionarios, contratistas y practicantes de la Administración Municipal de Plato Magdalena y demás personas que tengan acceso a información o tengan algún tipo de relación con la entidad.

3. ROLES Y RESPONSABILIDADES

El éxito de la Administración del Riesgo depende de diversos factores, pero la participación del Alcalde, Asesores, Secretarios y Jefes de Oficina permite que el proceso se desarrolle con mayor fluidez y efectividad, es por eso que se requiere la vinculación de la Alta Dirección y no solo involucrar al equipo técnico que hará el análisis y tratamiento del riesgo. por esto, es preciso identificar los actores que intervienen:

- ✓ **Alcalde Municipal:** Aprueba las directrices para la Administración del Riesgo en la Entidad y la asignación de rubros para implementaciones. El Alcalde Municipal es la responsable del fortalecimiento de la política de Administración del Riesgo.

- ✓ **Área de Control Interno:** aprueban las directrices para la administración del riesgo en la Administración Central Municipal de Plato. Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

- ✓ **Secretaría de Gobierno:** Líder del proceso en coordinación con el Área de Sistemas.

- ✓ **Secretarios de Despachos:** Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.

- ✓ **Servidores públicos y contratistas:** Ejecutar los controles y acciones definidas para la Administración de los Riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

4. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Administración Central Municipal de Plato adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, mediante el apoyo del Alcalde Municipal en conjunto con secretarios, funcionarios y contratistas es por ello que se comprometen a:

- Conocer y cumplir la política de seguridad de la información municipal.

- Replicar con sus equipos de trabajo fortaleciendo el trabajo mancomunado con la oficina de tecnología fortaleciendo la conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

- Aprobar la revisión frecuente de los procesos y procedimientos para la identificación de nuevos riesgos o control de los existentes.

- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto Para mitigar y lograr lo mencionado anteriormente, es necesario que sean asignados recursos humanos, presupuestales y tecnológicos que permitan cerrar las brechas detectadas y mejorar los controles existentes.

- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

5. 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

- ***Debilidad***: situación interna que la entidad puede controlar y que puede afectar su operación.

- ***Evaluación del riesgo***: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- ***Evitar el riesgo***: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

- ***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 (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

- ***Impacto***: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- ***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.

- ***Opciones de manejo***: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

- ***Plan de contingencia***: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.

- ***Probabilidad***: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- ***Procedimiento***: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- ***Proceso***: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- ***PTRSPI***: sigla de Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información.

- ***Riesgo***: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- ***Riesgo de corrupción***: posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- ***Riesgo inherente***: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- ***Riesgo institucional***: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

- Los riesgos que han sido clasificados como **estratégicos**: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.

- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.

- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- ***Riesgo residual***: nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- ***Valoración del riesgo***: establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

6. VALORACIÓN DE RIESGOS A LOS ACTIVOS DE INFORMACIÓN

6.1. Contexto de la entidad

La Administración Central Municipal de Plato se fortalece como una entidad territorial administrativa que garantizará la prestación de los servicios públicos que determina la ley, así como la construcción de las obras necesarias con calidad para el progreso del municipio; promover el desarrollo integral para mejorar la calidad de vida de la comunidad, administrar los recursos del Estado con transparencia, eficiencia y eficacia, con el desarrollo de planes, programas y proyectos encaminados al mejoramiento social , cultural , al ordenamiento y desarrollo de su territorio.

a. Contexto Interno Servicio

Protección a la información, protección al usuario y participación ciudadana.

b. Contexto de Seguridad y Privacidad de la Información

La información de la Administración Central Municipal de Plato, debe ser decisiva para el desarrollo de sus procesos, su correcto desempeño dentro de la política y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de salida de eventos de riesgo de seguridad de la información y que pudiese parecer un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

7. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1. Definición del Riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el Riesgo como la *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias"*.

De igual manera, el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información la Administración Central.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital, la estrategia de administración de riesgos para el flujo de la información en los procesos busca diseñar una metodología ligera enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información.

7.2 Riesgos de Seguridad Digital

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

7.3. Riesgos de Privacidad

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

7.4. Incidente de Seguridad de la Información

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como "*Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer Las actividades y vulnerar la seguridad*"; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información. Los factores de riesgos que se encuentran identificados dentro de la entidad están los siguientes:

Una de las acciones relevante es la identificación de riesgos sobre los activos de tecnologías de información frente a ciber amenazas, a partir de lo cual se define la siguiente matriz de riesgos:

Escenario de riesgo	Amenaza	Vulnerabilidad
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de operadores de botnets, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	Operadores de Botnets	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de Spayware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	Spyware/Malware	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de operadores botnets, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos	Operadores de Botnets	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
Afectación de la disponiblidad, integridad o confidencialidad de los servidores, por acción de Spayware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	Spyware/Malware	Falta o deficiencia en controles sobre la detección, revención, recuperación para proteger contra códigos maliciosos
Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de operadores botnets, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos	Operadores de Botnets	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de Spayware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos	Spyware/Malware	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de Spayware/Malware, debido a una falta o deficiencia en controles para los medios removibles	Spyware/Malware	Falta o deficiencia en controles para los medios removibles
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles de seguridad informática en la gestión de las redes	Hackers	Falta o deficiencia en controles de seguridad informática en la gestión de las redes

Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles sobre el acceso a redes y servicios en red	Hackers	Falta o deficiencia en controles sobre el acceso a redes y servicios en red
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de inicio de sesión	Hackers	Falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de inicio de sesión
Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información	Hackers	Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información	Atacante interno (insider)	Falta o deficiencia en controles que garantizen el adeucado análisis y especificación de requisitos de seguridad informática en los sistemas de información
Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información	Grupos criminales	Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
Afectación de la confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en el establecimiento y cumplimiento de una política sobre el uso de controles criptográficos	Hackers	Falta o deficiencia en el establecimiento y cumplimiento de una política sobre el uso de controles criptográficos
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de hackers, debido a una falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas	Hackers	Falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas	Atacante interno(insider)	Falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas

Afectación de la disponibilidad de los accesos a internet dedicados, por acción de hackers, debido a una falta o deficiencia en el mantenimiento y control de las redes, que dificulta la protección contra las amenazas y la gestión de seguridad de los sistemas y aplicaciones que usan la red	Hackers	Falta o deficiencia en el mantenimiento y control de las redes, que dificulta la protección contra las amenazas y la gestión de seguridad de los sistemas y aplicaciones que usan la red.
Afectación de la disponibilidad de los servidores y almacenamiento del correo electrónico, por acción de spam, debido a una alta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática	Spam	Falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática
Afectación de la integridad de los motores de bases de datos, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos.	Atacante interno (insider)	Falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos
Afectación de la integridad, disponibilidad y confidencialidad del servicio de correo electrónico institucional, por acción de phishing, debido a una alta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática	Phishing	Falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática
Afectación de la integridad, disponibilidad y confidencialidad de los servidores de bases de datos, por acción de atacante interno, debido a una falta o deficiencia en controles sobre el acceso a redes y servicios en red	Atacante interno(insider)	Falta o deficiencia en controles sobre el acceso a redes y servicios en red
Afectación de la integridad, disponibilidad y confidencialidad de los servidores integrados con la nube, por acción hackers, debido a una falta o deficiencia en controles sobre el acceso a redes y servicios en red	Hackers	Falta o deficiencia en controles sobre el acceso a redes y servicios en red
Afectación de la integridad, disponibilidad y confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos	Hackers	Falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos

De acuerdo con los riesgos identificados y las escalas propuestas por el Departamento Administrativo de la Función Pública, se realizó la actividad de valoración de los riesgos inherentes, así como de los riesgos residuales.

Se presenta el mapa de riesgos de los controles identificados de la aplicación de los controles a los riesgos inherentes, así como de los controles sobre los riesgos residuales identificados, en el que se identifican el conjunto de riesgos frente a la probabilidad de ocurrencia y el impacto de la materialización, tal como se puede evidenciar en la siguiente gráfica:

	Mapa de riesgo en seguridad informática frente a ciberamenazas						
Probabilidad de ocurrencia	Casi seguro	5					
	Probable	4					
	Posible	3		SD_3 SD_4	SD_7;SD_18	SD_19; SD_20; SD_21; SD_9; SD_10; SD_11	
	Improbable	2			SD_1; SD_2; SD_5; SD_6; SD_11; SD_12; SD_13; SD_14; SD_16; SD_17		
	Rara vez	1			SD_8; SD_15		
			1	2	3	4	5
			Insignificante	Menor	moderado	Mayor	Catastrofico
			Impacto de materialización				

No obstante, la organización es consciente que la gestión de riesgos de dinámica y que la revisión, actualización y reevaluación es parte de un ciclo que redunda en aportar al mejoramiento de la seguridad de la información corporativa.

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

Según lo expuesto en la guía para la administración del riesgo y el diseño de controles en entidades públicas por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de seguridad y privacidad de la información enfocado en la seguridad informática sobre los activos de tecnologías de información frente a ciber amenazas, para lo cual se realizan unas actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados.

En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de seguridad y privacidad de la información desde el enfoque de seguridad informática frente a ciber amenazas:

PLAN DE ACCION DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DESDE EL ENFOQUE DE SEGURIDAD INFORMATICA SOBRE LOS ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES FRENTE A CIBERAMENAZAS			
NO.	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE**	**TIEMPO**
1	Adquisición de Controles de Seguridad Informática frente a Ciber amenazas	Oficina de Recurso Humano / Secretaría de Gobierno	01/Feb/2024 31/Dic/2024
2	Implementación de Controles de Seguridad Informática frente a Ciber amenazas	Oficina de Recurso Humano / Secretaría de Gobierno	01/Feb/2024 31/Dic/2024
3	Seguimiento a la Operación de los Controles de Seguridad Informática frente a ciber amenazas	Oficina de Recurso Humano / Secretaría de Gobierno	01/Feb/2024 – 31/Dic/2024

BIBLIOGRAFÍA

- Cartillas de Administración Pública, Guía de Administración del Riesgo, Departamento Administrativo de la Función Pública, 2009.

- Guía Para la Administración del Riesgo, Departamento Administrativo de la Función Pública, 2011

- USAID Casals & Associates INC –EAFIT (2004) Modelo Estándar de Control Interno, 2004.

- Estatuto Anticorrupción. Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano”, 2012.