



Alcaldía de Medellín


**SECRETARIA DE INNOVACIÓN DIGITAL
SUBSECRETARÍA DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN
PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS
COMUNICACIONES**

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACIÓN
ENFOCADO EN LA SEGURIDAD INFORMATICA DE ACTIVOS DE
TECNOLOGÍAS DE INFORMACIÓN FRENTE A CIBERAMENAZAS**

**JUAN SEBASTIÁN GONZÁLEZ FLÓREZ
SECRETARIO DE INNOVACIÓN DIGITAL**

**JUAN GONZALO DUQUE BERRÍO
SUBSECRETARIO DE SERVICIOS DE TECNOLOGÍAS DE LA
INFORMACIÓN**

**ALCALDÍA DE MEDELLÍN
MEDELLIN – ANTIOQUIA
2022**

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

CONTENIDO

Hoja de autorizaciones.....	3
Revisiones y modificaciones	3
INTRODUCCIÓN.....	4
OBJETIVO.....	7
ALCANCE.....	7
AVANCES DE LA ENTIDAD EN EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	8
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN POR CATEGORÍAS FRENTE A CIBERAMENAZAS.....	14


2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

Hoja de autorizaciones

Elaboró:	Revisó:	Aprobó:
Amaury Rodríguez Oviedo Julian Andres Naranjo Londoño Carlos Andrés Arbeláez	Juan Gonzalo Duque Berrío	Juan Sebastian González Flórez
Líder Programa Unidad de Seguridad Informática	Subsecretario de Servicios de Tecnologías de la Información	Secretario de Innovación Digital

Revisiones y modificaciones

No. Revisió	Apartad o Modifica do	Página(s) Modifica da	Naturale za del Cambio	Motivo del cambio	Fecha de Vigencia	Elaboró	Aprobó

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

INTRODUCCIÓN

En Colombia se viene adelantando 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, título 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 cinco 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 la


2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

confidencialidad, integridad y disponibilidad de la información de las entidades del estado, y de los servicios que prestan al ciudadano.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecido en el decreto 612 de 2018, que en el artículo 1, señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción institucional, en el ámbito de aplicación del modelo integrado de planeación y gestión.

Así mismo, la resolución 0500 de Marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015. En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información enfocado en la seguridad informática frente a ciberamenazas de activos de tecnologías de información de la entidad.

2022	<p style="text-align: center;">Documento específico</p> <p style="text-align: center;">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	 Alcaldía de Medellín
Versión. 1		

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 ciberamenazas sobre activos de tecnologías de información y de las comunicaciones del Centro de Datos Corporativo.


2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

OBJETIVO

Establecer un marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información, sobre los activos de tecnologías de información que soportan la prestación de servicios digitales de la Entidad, desde el enfoque de la seguridad informática frente a ciberamenazas, mediante el cual se definen acciones para aportar al tratamiento de riesgos de seguridad y privacidad, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

ALCANCE

La planeación 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 de la plataforma tecnológica de la Alcaldía de Medellín frente a ciberamenazas, como un aporte a las acciones que realizará la entidad en torno a la seguridad y privacidad de la información institucional, teniendo en cuenta las capacidades y recursos disponibles, para mejorar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

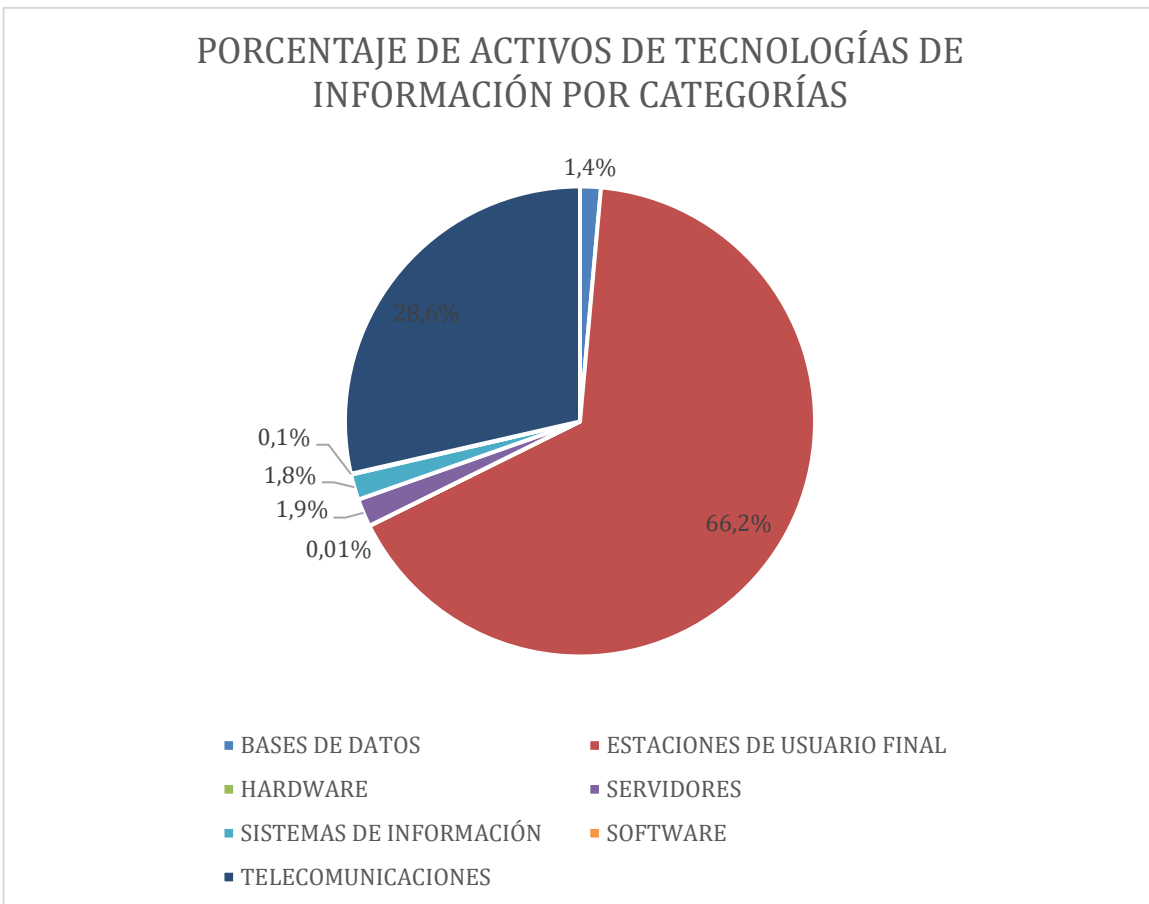
AVANCES DE LA ENTIDAD EN EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Secretaría de Innovación Digital ha priorizado abordar la gestión de riesgos de seguridad informática sobre los activos de tecnologías de información frente a ciberamenazas, en atención a la cantidad de procesos que realizan sus actividades apoyados en el uso de tecnologías de información y de las comunicaciones. Con cohorte al 17 de enero de 2021, la base de datos de activos de tecnologías de información registrada 21954 items de configuración registrados, de los cuales se consideraron 21700 como activos de tecnologías de información de interés para el análisis realizado, en atención al papel que juegan en la prestación de servicios institucionales.

Con el propósito de facilitar la identificación de los activos de tecnologías de información registrados, se han agrupado en un conjunto de categorías


CANTIDAD DE ELEMENTOS DE CONFIGURACIÓN POR CATEGORÍAS	
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN	PORCENTAJE DE ELEMENTOS DE CONFIGURACIÓN
ESTACIONES DE USUARIO FINAL	66,2%
TELECOMUNICACIONES	28,6%
SERVIDORES	1,9%
SISTEMAS DE INFORMACIÓN	1,8%
BASES DE DATOS	1,4%
SOFTWARE	0,1%
HARDWARE	0,01%
TOTAL	21.700

A partir de la agrupación se detalla que el 66.2% de los elementos de configuración se organizaron en el grupo de Estaciones de Usuario Final, que reúne los activos de tecnologías de información relacionados con equipos de cómputo, computadores portátiles y estaciones de ingeniería; y el 28.6% se organizaron en el grupo de Telecomunicaciones, así como el 1.9% en el grupo de servidores, tal como se puede evidenciar en la siguiente gráfica:




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


ID	Escenario de riesgo	Amenaza	Vulnerabilidad
SD_1	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	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		


SD_2	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	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
SD_3	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	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
SD_4	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	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
SD_5	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 fFalta o deficiencia en controles para los medios removiles	Spyware/Malware	[A.8.3.1] Falta o deficiencia en controles para los medios removiles
SD_6	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles de	Hackers	[A.13.1] Falta o deficiencia en controles de seguridad informática en la gestión de las redes

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		


	seguridad informática en la gestión de las redes		
SD_7	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	[A.9.1.2] Falta o deficiencia en controles sobre el acceso a redes y servicios en red
SD_8	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles que garantizan el procedimiento de ingreso seguro de inicio de sesión	Hackers	[A.9.4.2] Falta o deficiencia en controles que garantizan el procedimiento de ingreso seguro de inicio de sesión
SD_9	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 garantizan el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información	Hackers	[A.14.1.1] Falta o deficiencia en controles que garantizan el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
SD_10	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 garantizan el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información	Atacante interno(insider)	[A.14.1.1] Falta o deficiencia en controles que garantizan el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
SD_11	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en	Grupos criminales	[A.14.1.1] Falta o deficiencia en controles que garantizan el adecuado análisis y especificación de

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

	controles que garantizan el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información		requisitos de seguridad informática en los sistemas de información
SD_12	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	[A.10.1.1] Falta o deficiencia en el establecimiento y cumplimiento de una política sobre el uso de controles criptográficos
SD_13	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de hackers, debido a una falta o deficiencia en controles que garantizan la adecuada gestión de las vulnerabilidades técnicas	Hackers	[A.12.6.1] Falta o deficiencia en controles que garantizan la adecuada gestión de las vulnerabilidades técnicas
SD_14	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de atacantes internos, debido a una falta o deficiencia en controles que garantizan la adecuada gestión de las vulnerabilidades técnicas	Atacante interno(insider)	[A.12.6.1] Falta o deficiencia en controles que garantizan la adecuada gestión de las vulnerabilidades técnicas
SD_15	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	[A.13.1.1] 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
SD_16	Afectación de la disponibilidad de los servidores y almacenamiento del correo electrónico, por acción de spam, debido a una	Spam	[A.7.2.2] Falta o deficiencia en la toma de conciencia, educación y formación

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

	alta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática		en la seguridad informática
SD_17	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)	[A.12.4.1] Falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos
SD_18	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	[A.7.2.2] Falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática
SD_19	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)	[A.9.1.2] Falta o deficiencia en controles sobre el acceso a redes y servicios en red
SD_20	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	[A.9.1.2] Falta o deficiencia en controles sobre el acceso a redes y servicios en red
SD_21	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	Hackers	[A.12.4.1] Falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		


	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, a partir de la cual se obtuvo el plan de tratamiento de riesgos de la vigencia anterior. A continuación se presenta el mapa de riesgos producto de la aplicación 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 redundo en aportar al mejoramiento de la seguridad de la información corporativa.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN POR CATEGORÍAS FRENTE A CIBERAMENAZAS

2022	Documento específico PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 Alcaldía de Medellín
Versión. 1		

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 ciberamenazas, 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 ciberamenazas:

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 Ciberamenazas	Líder de Implementación de Controles de Seguridad Informática Líder de Gestión a Incidentes de Seguridad Informática	01/Feb/2022 – 31/Dic/2022
2	Implementación de Controles de Seguridad Informática frente a Ciberamenazas	Líder de Implementación de Controles de Seguridad Informática Líder de Gestión a Incidentes de Seguridad Informática	01/Feb/2022 – 31/Dic/2022
3	Seguimiento a la Operación de los Controles de Seguridad Informática frente a ciberamenazas	Líder de Implementación de Controles de Seguridad Informática Líder de Gestión a Incidentes de Seguridad Informática	01/Feb/2022 – 31/Dic/2022

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo corporativo que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.