Alcaldía de Medellín

SECRETARÍA DE INNOVACIÓN DIGITAL

SUBSECRETARÍA DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

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

JUAN SEBASTIÁN GONZÁLEZ FLÓREZ
SECRETARIO DE INNOVACIÓN DIGITAL

JULIANA RAMÍREZ GÓMEZ
SUBSECRETARIA DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

ALCALDÍA DE MEDELLÍN
MEDELLÍN – ANTIOQUIA
2021

SECRETARÍA DE INNOVACIÓN DIGITAL

SUBSECRETARÍA DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

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

AMAURY RODRÍGUEZ OVIEDO
JULIÁN ANDRÉS NARANJO LONDOÑO
CARLOS ANDRÉS ARBELÁEZ VELÁSQUEZ
UNIDAD DE SEGURIDAD INFORMÁTICA

CARLOS BOTERO LONDOÑO
UNIDAD DE INFRAESTRUCTURA

JULIANA RAMÍREZ GÓMEZ
SUBSECRETARIA DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

ALCALDÍA DE MEDELLÍN
MEDELLÍN – ANTIOQUIA
2021

CONTENIDO

HOJA DE AUTORIZACIONES

Elaboró:	Revisó:	Aprobó:
Amaury Rodríguez Oviedo **Lubián de Jesús Cartagena** **Carlos Andrés Arbeláez**	**Juliana Ramírez Gómez**	**Juan Sebastián González**
Líder Programa Unidad de Seguridad Informática.	Subsecretaria de Servicios de Tecnologías de Información.	Secretario de Innovación Digital.

REVISIONES Y MODIFICACIONES

No. Revisión	Apartado Modificado	Página(s) Modificada	Naturaleza del Cambio	Motivo del cambio	Fecha de Vigencia	Elaboró	Aprobó

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

Así mismo, con el propósito de fortalecer la seguridad de la información en Colombia, el Consejo Nacional de Política Económica y Social –CONPES- expidió el documento 3854, denominado “Política Nacional de Seguridad Digital”, la cual tiene como objetivo el fortalecimiento de las capacidades de las múltiples partes

interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

La apuesta del Estado Colombiano se aborda en un marco de cooperación, colaboración y asistencia, encaminada a contribuir al crecimiento de la economía digital nacional, lo que a su vez, impulsaría una mayor prosperidad económica y social en el país. Los riesgos de seguridad digital a los que hace alusión la política, son definidos por el Departamento Administrativo de la Función Pública –DAFP-, como la combinación de amenazas y vulnerabilidades en el entorno digital.

El CONPES 3854 define entorno digital como el ambiente tanto físico, como virtual, sobre el cual se soporta la economía digital; siento ésta, una economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicaciones, equipos de hardware, servicios de procesamiento y tecnologías web.

La implementación del habilitador de seguridad de la información, toma como sustento los lineamientos propuestos por el Ministerio de Tecnologías de Información y de las Comunicaciones, a través del Modelo de Seguridad y Privacidad de la Información – MSPI-, quien 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.

El Modelo de Seguridad y Privacidad de la Información toma como sustento el estándar NTC ISO 27001:2013 o Sistema de Gestión de Seguridad de la Información y los principios legales de la Ley 1712 de 2014; resaltando que tanto el estándar en mención, como el modelo, conciben obligatorio la identificación, valoración, tratamiento y gestión de los riesgos de seguridad, coincidiendo con los objetivos específicos de la política de Seguridad Digital, en cuanto al establecimiento de un marco institucional para la seguridad digital, consistente con un enfoque de gestión de riesgos, enfatizando en la implementación por parte del gobierno nacional a un modelo de gestión de riesgos de seguridad digital.

En atención a lo anterior, el Departamento Administrativo de la Función Pública expide la guía para la administración del riesgo y el diseño de controles en entidades públicas para los riesgos de gestión, corrupción y seguridad digital; en el que se propone una metodología para la administración de riesgos y en particular, expide el modelo de gestión de riesgos de seguridad digital, como un documento anexo a la guía.

Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información.

OBJETIVO

Presentar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Alcaldía de Medellín, en atención a lo dispuesto en el decreto 612 de 2018, como parte activa de la Política de Seguridad de la Información adoptada por la entidad; mediante el cual se definen las acciones para fortalecer las capacidades institucionales en el tratamiento de los riesgos de seguridad y privacidad de la información en la entidad.

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Alcaldía de Medellín, para la vigencia 2021, está orientado a gestionar los riesgos de seguridad digital asociados a la plataforma tecnológica y servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades asociadas al modelo de operación por procesos adoptados en la entidad.

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

La Alcaldía de Medellín ha priorizado el proceso de tecnologías de información y de las comunicaciones, en atención al impacto que tiene el mismo sobre los procesos estratégicos, misionales y de apoyo; ya que actualmente, desde la secretaría de Innovación Digital se coordinan todas las actividades de adquisición, implementación y mantenimiento de tecnologías de información y de las comunicaciones para la entidad, por lo cual, una afectación a este proceso, tendrían un impacto alto para el logro de los objetivos institucionales.

Sin lugar a dudas, el valor de la seguridad informática de cualquier organización debe redundar en la protección de activos de tecnologías de información, de allí la relevancia de contar con la información que se toma como base para realizar las actividades orientadas a la identificación de riesgos y los planes de tratamiento de datos requeridos para mantener un nivel de riesgo aceptable.

Para facilitar la identificación de activos de tecnologías de información, se tomó como base la información de la denominada CMDB o base de datos de administración de la configuración registrada en la herramienta Aranda, con cohorte al 15 de marzo de 2020, en la que se identificaron 19.860 CI o Elementos de Configuración Registrados, de los cuales, a partir de la identificación de categorías registradas, se realizó una revisión manual y se seleccionaron aquellos elementos de configuración que coincidían de manera más precisa con elementos

asociados a las tecnologías de información, descartando aquellos elementos que se encuentran asociados a categorías como Aire Acondicionado, Dispensadores de Turnos, entre otras.

A partir de la revisión de las 28 categorías definidas en la herramienta Aranda, se seleccionaron 18, que a su vez, consolidan el total de los elementos de configuración, de los cuales se puede resaltar que 82.9% de ellos hacen referencia a Equipos de Cómputo, 3.6% a Switches y el 2.4% a Servidores, tal como se presenta en la siguiente tabla:

CANTIDAD DE ELEMENTOS DE CONFIGURACIÓN POR CATEGORÍAS	
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN	**PORCENTAJE DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN**
ACCESOS	0,6%
ALMACENAMIENTO	0,3%
APLICACIONES	0,5%
APPLIANCE	0,2%
BANDA ANCHA	0,2%
BASES DE DATOS ORACLE	0,8%
BASES DE DATOS SQL	1,3%
DEDICADOS	0,0%
DISPOSITIVOS	0,6%
ESTACIONES DE INGENIERIA	1,5%
PC´S	73,3%
PORTATILES	9,5%
PUNTOS DE ACCESO INALAMBRICO AP´S	1,8%
RADIO ENLACES	1,1%
SERVIDORES	2,4%
SISTEMAS DE INFORMACIÓN	2,1%
SOFTWARE	0,1%
SWITCHES	3,6%

No obstante, estas categorías fueron revisadas y analizadas, y a partir de ese proceso, se definieron 7 grupos que a su vez consolidan un conjunto de categorías, tal como se presenta en la siguiente tabla:

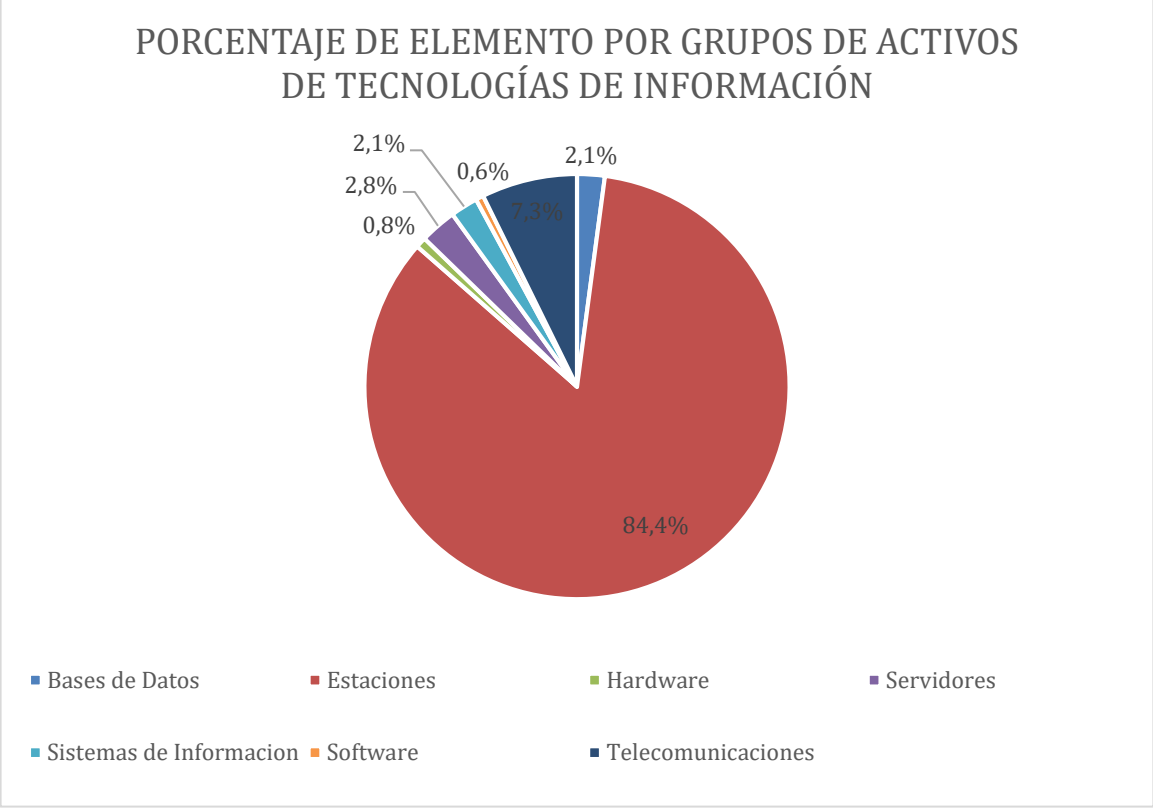
CANTIDAD DE ELEMENTOS DE CONFIGURACIÓN POR CATEGORÍAS	
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN	**CANTIDAD DE ELEMENTO DE CONFIGURACIÓN**
BASES DE DATOS	2
ESTACIONES	3
HARDWARE	2
SERVIDORES	2
SISTEMAS DE INFORMACION	1
SOFTWARE	2
TELECOMUNICACIONES	6
TOTAL	**18**

A cada grupo se le distribuyeron las categorías seleccionadas, con el objetivo de facilitar la identificación de riesgos, su valoración, así como los controles necesarios, tal como se puede evidenciar en la siguiente tabla:

PORCENTAJE DE ELEMENTOS DE CONFIGURACIÓN POR CATEGORÍAS Y GRUPOS		
GRUPO DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN	**PORCENTAJE DE ACTIVOS DE TECNOLOGÍA DE INFORMACIÓN**	**PORCENTAJE DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN**
BASES DE DATOS	0,8%	0,8%
BASES DE DATOS	1,3%	1,3%
TOTAL DE ELEMENTOS EN BASES DE DATOS		**2,1%**
ESTACIONES	1,5%	1,5%
ESTACIONES	73,3%	73,3%
ESTACIONES	9,5%	9,5%
TOTAL DE ELEMENTOS EN ESTACIONES		**84,4%**
HARDWARE	0,2%	0,2%
HARDWARE	0,6%	0,6%
TOTAL DE ELEMENTOS EN HARDWARE		**0,8%**

PORCENTAJE DE ELEMENTOS DE CONFIGURACIÓN POR CATEGORÍAS Y GRUPOS		
GRUPO DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN	**PORCENTAJE DE ACTIVOS DE TECNOLOGÍA DE INFORMACIÓN**	**PORCENTAJE DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN**
SERVIDORES	0,3%	0,3%
SERVIDORES	2,4%	2,4%
TOTAL DE ELEMENTOS EN SERVIDORES		**2,8%**
SISTEMAS DE INFORMACION	2,1%	2,1%
TOTAL DE ELEMENTOS EN SISTEMAS DE INFORMACIÓN		**2,1%**
SOFTWARE	0,5%	0,5%
SOFTWARE	0,1%	0,1%
TOTAL DE ELEMENTOS EN SOFTWARE		**0,6%**
TELECOMUNICACIONES	0,6%	0,6%
TELECOMUNICACIONES	0,2%	0,2%
TELECOMUNICACIONES	0,0%	0,0%
TELECOMUNICACIONES	1,8%	1,8%
TELECOMUNICACIONES	1,1%	1,1%
TELECOMUNICACIONES	3,6%	3,6%
TOTAL DE ELEMENTOS EN TELECOMUNICACIONES		**7,3%**

A partir de la agrupación se detalla que el 84.4% de los elementos de configuración se organizaron en el grupo de Estaciones, que reúne los activos de tecnologías de información relacionados con equipos de cómputo, computadores portátiles y estaciones de ingeniería; y el 7.3% se organizaron en el grupo de Telecomunicaciones, así como el 2.8% en el grupo de Servidores, tal como se puede evidenciar en la siguiente gráfica:



Una vez se consolidó la información, se alinearon los grupos definidos con las categorías definidas en la versión 1.0 de la guía de clasificación de activos de información, publicada por el Ministerio de Tecnologías de Información y de las Comunicaciones, a partir de lo cual, se consolida el siguiente inventario que precisa información sobre el proceso, tipo de activo según la guía del Ministerio de Tecnologías de Información y de las Comunicaciones, grupo de activo y tipo de activo según la base de datos de elementos de configuración y el porcentaje de elementos que la conforman:

INVENTARIO DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN					
PROCESO	**No.**	**TIPO DE ACTIVO SEGÚN GUÍA MINTIC**	**AGRUPACIÓN DE ACTIVO**	**TIPO DE ACTIVO EN LA CMDB**	**PORCENTAJE**
TIC	1	HARDWARE	ESTACION DE USUARIO	PC´S	35,79%
TIC	2	HARDWARE	ESTACION DE USUARIO	PORTATILES	4,64%
TIC	3	HARDWARE	ESTACION DE USUARIO	ESTACIONES DE INGENIERIA	0,73%
TIC	4	COMPONENTES DE RED	TELECOMUNICACIONES	PUNTOS DE ACCESO INALAMBRICO AP´S	0,87%
TIC	5	COMPONENTES DE RED	TELECOMUNICACIONES	RADIO ENLACES	0,54%
TIC	6	COMPONENTES DE RED	TELECOMUNICACIONES	SWITCHES	1,75%
TIC	7	COMPONENTES DE RED	TELECOMUNICACIONES	DISPOSITIVOS	0,30%
TIC	8	COMPONENTES DE RED	TELECOMUNICACIONES	TELÉFONOS	16,49%
TIC	9	SOFTWARE	SOFTWARE	SOFTWARE	0,04%
TIC	10	SOFTWARE	SOFTWARE	APLICACIONES	0,25%
TIC	11	INFORMACION	BASE DE DATOS	BASES DE DATOS SQL	0,65%
TIC	12	INFORMACION	BASE DE DATOS	BASES DE DATOS ORACLE	0,38%
TIC	13	SERVICIOS	SISTEMA DE INFORMACIÓN	SISTÉMAS DE INFORMACIÓN	1,02%
TIC	14	SERVICIOS	SERVIDORES	ALMACENAMIENTO	0,16%
TIC	15	SERVICIOS	SERVIDORES	SERVIDORES	1,19%
TIC	16	SERVICIOS	CONECTIVIDAD	ACCESOS	0,29%
TIC	17	SERVICIOS	CONECTIVIDAD	BANDA ANCHA	0,08%
TIC	18	SERVICIOS	CONECTIVIDAD	DEDICADOS	0,02%
TIC	19	SERVICIOS	SERVICIOS	CORREO ELECTRÓNICO CORPORATIVO	34,80%
TIC	20	INSTALACIONES	INSTALACIONES	CENTRO DE DATOS CORPORATIVO	0,01%

Aunque la base de datos del inventario de activos de tecnologías de información consolidado subyace de la información extraída de la base de datos de la CMDB de la herramienta ARANDA, se concluyó que dos grupos importantes que no están

incluidos explícitamente en la CMDB se debían incluir, estos grupos son: El grupo de Servicios y el de Instalaciones.

El grupo de Servicios se define para incluir prioritariamente el correo electrónico corporativo, ya que sobre este servicio se utilizan un número considerable de cuentas, que se convierten en elementos importantes para la evaluación de riesgos; de igual manera, se incluye el centro de datos corporativos, por ser el lugar central donde se aloja toda la infraestructura de tecnologías de información.

A partir de la identificación, se procede con la valoración de los activos de tecnologías de información, la cual se realiza a nivel de tipos de elementos frente a criterios como la confidencialidad, la integridad y la disponibilidad; tomando como referencia la criticidad del activo frente a estos criterios, los cuales, se usaron posteriormente para definir el tipo de criticidad del activo de tecnologías de información.

Es importante mencionar que la valoración del activo se debe realizar por el propietario del activo, ya que es desde ese contexto donde se puede construir el valor que tiene el activo de tecnología de información frente a la organización, así como el valor que tiene la información almacenada en dicho activo de información y el valor de sus servicio en términos de la operación organizacional.

A continuación, se presenta la tabla de valoración de los activos de tecnologías de información definiendo, por cada categoría y la cantidad, la valoración desde

los 3 criterios definidos y con base en ellos, establecer la criticidad del activo en la organización.

VALORACIÓN DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN				
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**CRITICIDAD**
PC´S	1	1	1	BAJA
PORTATILES	1	1	1	BAJA
ESTACIONES DE INGENIERIA	1	1	1	BAJA
PUNTOS DE ACCESO INALAMBRICO AP´S	2	1	2	MEDIA
RADIO ENLACES	2	1	2	MEDIA
SWITCHES	1	1	2	BAJA
DISPOSITIVOS	1	1	2	BAJA
TELÉFONOS	2	2	1	ALTA
SOFTWARE	1	1	1	BAJA
APLICACIONES	3	2	2	ALTA
BASES DE DATOS SQL	3	3	2	ALTA
BASES DE DATOS ORACLE	3	3	2	ALTA
SISTÉMAS DE INFORMACIÓN	3	2	2	ALTA
ALMACENAMIENTO	3	2	2	ALTA
SERVIDORES	2	2	2	MEDIA
ACCESOS	1	1	2	BAJA
BANDA ANCHA	1	1	2	BAJA
DEDICADOS	2	1	2	MEDIA
CORREO ELECTRÓNICO CORPORATIVO	3	2	3	ALTA
CENTRO DE DATOS CORPORATIVO	3	2	3	ALTA

La identificación y valoración de activos es una de las actividades más relevantes para la organización y se convierte en un insumo fundamental para la identificación de riesgos de seguridad informática, sin embargo, el primer factor

relevante para la identificación de los mismos es el alcance, para lo cual se ha definido que la evaluación de riesgos realizada es frente a ciberamenazas.

A partir de las agrupaciones realizadas se inició el proceso de identificación de riesgos, para lo cual se identifican amenazas y vulnerabilidades. No obstante, sobre un grupo de activos se pueden identificar diferentes riesgos, tal como se evidencia en la siguiente tabla:

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**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.	SERVIDORES	Operadores de Botnets	[A.12.2.1] 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 Spyware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	SERVIDORES	Spyware/Malware	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
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	ESTACIONES DE USUARIO	Operadores de Botnets	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos

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 Spyware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	ESTACIONES DE USUARIO	Spyware/Malware	[A.12.2.1] 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 Spyware/Malware, debido a una falta o deficiencia en controles para los medios removibles.	ESTACIONES DE USUARIO	Spyware/Malware	[A.8.3.1] 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	SERVIDORES	Hackers	[A.13.1] Falta o deficiencia en controles de seguridad informática en la gestión de las redes

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
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.	SERVIDORES	Hackers	[A.9.1.2] 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.	SERVIDORES	Hackers	[A.9.4.2] 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.	SISTEMAS DE INFORMACIÓN	Hackers	[A.14.1.1] 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 atacantes internos, 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	SISTEMAS DE INFORMACIÓN	Atacante interno (insider)	[A.14.1.1] Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de grupos criminales, 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.	SISTEMAS DE INFORMACIÓN	Grupos criminales	[A.14.1.1] 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	SISTEMAS DE INFORMACIÓN	Hackers	[A.10.1.1] 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.	SERVIDORES	Hackers	[A.12.6.1] 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.	SERVIDORES	Atacante interno(insider)	[A.12.6.1] Falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas.

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
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.	CONECTIVIDAD	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.
Afectación de la disponibilidad de los servidores y almacenamiento del correo electrónico, por acción de spam, debido a	SERVICIOS	Spam	[A.12.2.1] Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.

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.	INFORMACIÓN	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
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.	SERVICIOS	Phishing	[A.7.2.2] Falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática

A partir de la identificación de riesgos sobre los activos de tecnologías de información frente a ciberamenazas y de acuerdo con la versión 3.0.1 de la guía de gestión de riesgos publicada por el Ministerio de Tecnologías de Información y Comunicaciones, se realiza la valoración del riesgo inherente, para lo cual se toma como concepto base, la inexistencia de controles y la probabilidad de ocurrencia de un evento, así como el impacto de la ocurrencia, a partir de los cuales, se define la calificación del riesgo inherente.

No obstante, para realizar dicha valoración se toman como referentes unas escalas de valoración que permiten unificar los criterios de valoración y hacerlos comparables, tal como la escala para calificar la probabilidad de ocurrencia de un riesgo, en la que se define un nivel del riesgo, un descriptor, una descripción del criterio y una orientación para la evaluación de la probabilidad en torno a unas

frecuencias como punto de partida para el análisis, tal como se evidencia en la siguiente tabla:

Tabla 2. Criterios parar calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Así mismo se define una escala para la valoración del impacto de la materialización de un riesgo sobre la organización, la cual contempla un nivel y las consecuencias posibles que permiten definir la criticidad de ese impacto, tal como se evidencia en la siguiente tabla:

Nivel	Consecuencias
Catastrófico	• Intervención por parte de un ente de control u otro ente regulador. • Perdida de información crítica para el proceso que no se puede recuperar. • Incumplimiento en las metas y objetivos del proceso, afectando el plan de desarrollo. • Imagen Institucional afectada en el orden territorial, regional o nacional por la no prestación de los servicios a los usuarios o ciudadanos. • Criterio direccionador del proceso.

Mayor	• Intervención por parte de un ente de control u otro ente regulador. • Perdida de información crítica para el proceso que no se puede recuperar. • Incumplimiento en las metas y objetivos del proceso, afectando el presupuesto del proceso. • Imagen Institucional afectada en el orden territorial, regional o nacional, por retrasos en la prestación de los servicios a los usuarios o ciudadanos. • Criterio direccionador del proceso.
Moderado	• Intervención por parte de un ente de control u otro ente regulador. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios o ciudadanos. • Reclamaciones o quejas de los usuarios o ciudadanos, que podrían implicar una denuncia o demanda. • Reprocesos de actividades y aumento de la carga operativa. • Criterio del direccionador del proceso.
Menor	• No hay intervenciones de los entes de control u otro ente regulador. • No se afecta la imagen institucional. • No hay incumplimiento de objetivos y metas del proceso. • Hay reclamaciones o quejas de los usuarios o ciudadanos. • Hay reproceso de actividades y aumento en la carga operativa. • Criterio direccionador del proceso.
Insignificante	• No hay intervenciones de los entes de control u otro ente regulador. • No se afecta la imagen institucional. • No hay incumplimiento de objetivos y metas del proceso. • No hay reclamaciones o quejas de los usuarios o ciudadanos. • Criterio direccionador del proceso.

A partir de esas escalas de valoración se define un valor numérico para representar la criticidad en la probabilidad o en el impacto, de tal manera que se pueda obtener una calificación, a partir de la combinación de la probabilidad de ocurrencia y el impacto de ocurrencia, tal como se evidencia en la siguiente tabla:

Probabilidad	
Descripción	**Puntaje**
RARA VEZ	1
IMPROBABLE	2
POSIBLE	3
PROBABLE	4
CASI SEGURO	5

Impacto	
Descripción	**Puntaje**
INSIGNIFICANTE	1
MENOR	2
MODERADO	3
MAYOR	4
CATASTROFICO	5

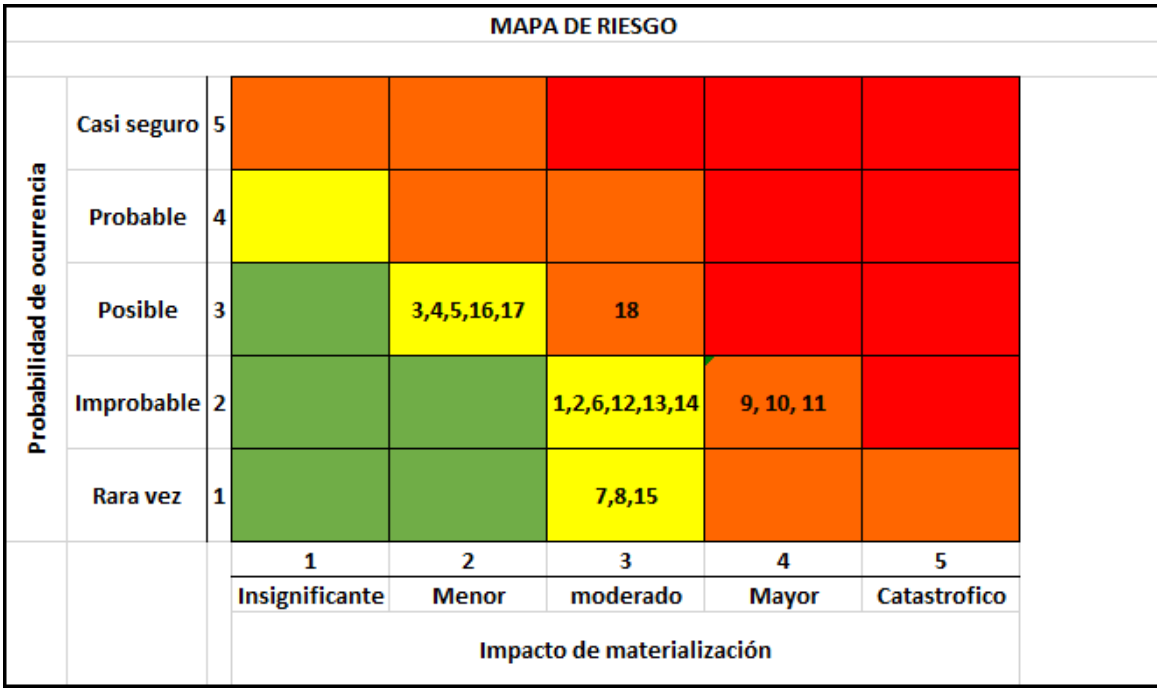
Los puntajes definidos se utilizan como factores de valoración, y la combinación de ellos ayuda a definir los escenarios de valoración de riesgos y su priorización, para lo cual se toma como referencia la siguiente tabla:

VALORACIÓN DE RIESGOS A PARTIR DE LA PROBABILIDAD DE OCURRENCIA Y EL IMPACTO			
Probabilidad	**Impacto**	**Nivel Riesgo**	**Zona de Calor**
1	1	1	BAJO
1	2	2	BAJO
1	3	3	MODERADO
1	4	4	ALTO
1	5	5	ALTO
2	1	2	BAJO
2	2	4	BAJO
2	3	6	MODERADO
2	4	8	ALTO
2	5	10	EXTREMO
3	1	3	BAJO
3	2	6	MODERADO
3	3	9	ALTO
3	4	12	EXTREMO

VALORACIÓN DE RIESGOS A PARTIR DE LA PROBABILIDAD DE OCURRENCIA Y EL IMPACTO			
Probabilidad	**Impacto**	**Nivel Riesgo**	**Zona de Calor**
3	5	15	EXTREMO
4	1	4	MODERADO
4	2	8	ALTO
4	3	12	ALTO
4	4	16	EXTREMO
4	5	20	EXTREMO
5	1	5	ALTO
5	2	10	ALTO
5	3	15	EXTREMO
5	4	20	EXTREMO
5	5	25	EXTREMO

De acuerdo con estas escalas, se realizó la actividad de valoración de los riesgos inherentes, de acuerdo con las orientaciones del Ministerio de Tecnologías de Información y de las Comunicaciones y del Departamento Administrativo de la Función Pública; 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 presentan 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:



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.

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

La planeación en el tratamiento de riesgos de seguridad frente a ciberamenazas se realizará sobre el conjunto de categorías que se han identificado sobre la base de datos de elementos de configuración existente y adicionando los servicios asociados al correo electrónico corporativo y las instalaciones de procesamiento existentes, que tienen una representación porcentual en cantidad, de acuerdo con la siguiente tabla:

CATEGORÍA	PORCENTAJE
ESTACION DE USUARIO	41,16%
TELECOMUNICACIONES	19,96%
SOFTWARE	0,29%
BASE DE DATOS	1,03%
SISTEMA DE INFORMACIÓN	1,02%
SERVIDORES	1,35%
CONECTIVIDAD	0,39%
SERVICIOS	34,80%
INSTALACIONES	0,01%

El diseño de planes de tratamiento está orientado a partir de las guías sugeridas por el Ministerio de Tecnologías de Información y de las Comunicaciones y el Departamento Administrativo de la Función Pública, a partir de las cuales se

presentan a continuación, las etapas más relevantes y conducentes no solo a la revisión de los riesgos ya identificados, sino también a la revaloración de los mismos, así como a la identificación de nuevos riesgos, que son un escenario en continuo cambio, por la dinámica de cambio de las infraestructuras, los contextos de uso, de las vulnerabilidades e incluso de las mismas amenazas.

El plan describe las actividades más relevantes a realizar en el período 2021, de tal manera que orienten el quehacer de la organización para afrontar los riesgos frente a ciberamenazas, tal como se refleja en la siguiente tabla:

NO.	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	TIEMPO
1	Sensibilización, Socialización y Capacitación a responsables de los Activos de Tecnologías Información, sobre el proceso de identificación, valoración, tratamiento y gestión de riesgos frente a ciberamenazas.	Líder de Implementación de Controles de Seguridad Informática.	01/May/2021 31/Dic/2021
2	Actualización de la valoración de Riesgos de seguridad informática frente a ciberamenazas.	Líder de Implementación de Controles de Seguridad Informática. Líder de Gestión de Incidentes de Seguridad Informática.	01/Jul/2021 30/Nov/2021
3	Identificación y valoración de nuevos Riesgos asociados a cada Categoría frente a Ciberamenazas.	Líder de Implementación de Controles de Seguridad Informática. Líder de Gestión de Incidentes de Seguridad Informática.	01/Oct/2021 31/Nov/2021
4	Evaluación de los Controles de seguridad informática Implementados frente a ciberamenazas.	Líder de Implementación de Controles de Seguridad Informática. Líder de Gestión de Incidentes de Seguridad Informática.	01/Oct/2021 31/Nov/2021
5	Actualizar el Plan de Tratamiento de Riesgos frente a Ciberamenazas.	Líder de Implementación de Controles de Seguridad Informática.	01/Nov/2021 31/Dic/2021

El desarrollo de las actividades estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; mientras que la valoración de los riesgos y sus tratamientos estará delimitada por el requerido apoyo de la alta dirección, en cuanto al apetito de riesgo corporativo que han adoptado, para afrontar el desarrollo y cumplimiento de las actividades planificadas.