ALCALDÍA MAYOR
DE BOGOTÁ D.C.

BOGOTÁ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

TABLA DE CONTENIDO

INTRODUCCIÓN

Las tendencias tecnológicas de los últimos años, han permitido crear de manera exponencial cantidades de información que jamás en la historia de la humanidad se habían creado, transportado, transformado o compartido, cambiando la manera de ver las cosas por parte de todos nosotros. Particularmente en las entidades del estado, se hace necesario contar con la conciencia del poder de la información, el alcance que tiene la misma y principalmente la entrega oportuna que se debe dar a la ciudadanía.

En la Secretaría de Seguridad, Convivencia y Justicia se cuenta con gran volumen de información, relevante para el Distrito, manejada física, digital y electrónicamente, en su mayoría con el propósito de dar cumplimiento a los objetivos de la entidad, requiriendo utilizar mecanismos adecuados para cuidar el derecho a la intimidad personal, familiar y al buen nombre de todos los beneficiarios de la entidad, permitiendo el acceso a los documentos públicos y evitando el acceso a los que se consideren reservados o confidenciales.

Para lograr la toma de decisiones con base en información de altos estándares de calidad, en materia de política y gestión de Seguridad, Convivencia y Acceso a la Justicia, que permita tomar decisiones, resolver problemas y prestar los servicios a los ciudadanos y funcionarios de la entidad, es necesario que esta sea real, oportuna y de acceso a las personas o procesos que lo requieran.

Teniendo en cuenta lo anterior, en el marco internacional la norma ISO 31000 ayuda a establecer un Sistema de Gestión de Riesgos que permite identificar, divulgar y medir los posibles incumplimientos a los objetivos institucionales de la entidad mediante la identificación de los riesgos asociados a la información. Lo anterior permite reducir las falencias propias de la información a través de la evaluación e implementación de los controles adecuados que permitan mitigar las afectaciones negativas a la organización.

Basados en lo anterior y teniendo en cuenta lo definido en el artículo 1 del decreto 612 de 2018, donde se establece que las entidades del estado deben integrar los planes institucionales y estratégicos y publicarlos a más tardar el 31 de enero de cada año, la Secretaría Distrital de Seguridad, Convivencia y Justicia establece el

respectivo plan para el tratamiento de los riesgos de seguridad digital, mediante el cual se realizará la identificación, clasificación, valoración y tratamiento de los riesgos de seguridad digital, las amenazas y vulnerabilidades a los que están expuestos los activos de información, para posteriormente definir los respectivos controles que mitigan la materialización de los riesgos, lo anterior alineado al cumplimiento de la Política de Seguridad y privacidad de la Información de la Secretaría de Seguridad, Convivencia y Justicia.

OBJETIVOS

Objetivo General

Establecer el plan que permita realizar el tratamiento de los riesgos de seguridad digital identificados en los procesos de la entidad.

Objetivos Específicos

El Plan de Tratamiento de Riesgos de Seguridad Digital da cumplimiento a uno de los objetivos específicos de la Política de Seguridad y privacidad de la Información, a través de los siguientes objetivos específicos:

1. Identificar los riesgos de Seguridad Digital en todos los procesos de la entidad.
2. Establecer el plan de tratamiento de riesgos de seguridad digital.
3. Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad digital de la Entidad.

GLOSARIO DE TÉRMINOS

- **Activo (CONPES 3854:2016, pág.56):** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información

física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - 2018).

- **Activo cibernético:** En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).
- **Amenaza cibernética**: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).
- **Aceptación del riesgo:** Decisión de asumir el riesgo (Guía ISO/IEC 73:2002)
- **Análisis del riesgo:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).
- **Apetito de riesgo:** Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar. (Componente COSO ERM II)
- **Ataque cibernético:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).
- **CCOC:** Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.
- **CERT:** Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).
- **Cibercrimen (Delito cibernético):** Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).
- **Ciberdefensa:** Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).
- **Ciberseguridad:** Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación,

confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

- **Ciberterrorismo:** Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas. (CONPES 3854, pág. 88).
- **Ciberdelincuencia:** Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).
- **Ciberdelito/Delito cibernético:** Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).
- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009). Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).
- **Cibernético**: Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Diccionario de la lengua española).
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Confidencialidad:** propiedad que determina que la información no este disponible ni sea revelada a individuos, entidades o procesos no autorizados (NTC 5411-1:2006)
- **Control:** medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - 2018).
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (NTC 5411-1:2006)
- **Entorno digital:** Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la 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 comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

- **Entorno digital abierto:** En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).
- **Evaluación del control:** Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).
- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).
- **Evento de seguridad de la información:** Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).
- **Evitar el riesgo:** Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).
- **Evento**: Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).
- **Frecuencia:** Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (NTC ISO 31000:2011).
- **Gestión de riesgos de seguridad digital:** Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).
- **ICC:** Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su

perturbación o destrucción tendría un grabe impacto sobre los servicios esenciales.

- **Identificación del riesgo:** Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).
- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
- **Impacto:** se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos. (NTC 5411-1:2006)
- **Inventario de activos:** Sigla en inglés: *Assets inventory*. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).
- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).
- **Línea estratégica:** define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **Múltiples partes interesadas:** El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades. (CONPES 3854, pág. 29).

- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).
- **Parte involucrada:** Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).
- **Política de administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.
- **Primera línea de defensa:** a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.
- **Probabilidad:** Oportunidad de que algo suceda. (NTC ISO 31000:2011).
- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar el riesgo. (ISO 31000:2011)
- **Reducción del riesgo:** Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).
- **Responsabilidad:** Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales. (CONPES 3854, pág. 25).
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).
- **Riesgos de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas. (Guía para la Administración del riesgo y el diseño de controles en entidades

públicas - 2018).

- **Riesgo residual:** Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).
- **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).
- **Segunda línea de defensa:** asiste y guía a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).
- **Servicios Esenciales:** son los necesarios para el mantenimiento de las funciones sociales básicas la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del estado y las administraciones públicas. (Tomado del documento ICC del CCOC).
- **SGC:** Sistema de gestión de calidad.
- **SGSI:** Sistema de gestión de seguridad de la información.
- **Sistema para la gestión del riesgo:** Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).
- **Tercera línea de defensa:** provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con

sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno o Auditoria Interna.

- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - 2018).
- **Tratamiento al riesgo:** es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos. (Norma Técnica Colombiana ISO-IEC 27000)
- **Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

MARCO LEGAL

- **Decreto 1499 de 2017**: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 y se establece el MIPG - Presidencia de la Republica.
- **Artículo 73 de la Ley 1474 de 2011**: Relacionado con la prevención de los riesgos de corrupción, - mapa de riesgos de corrupción. - Secretaría de Trasparencia de la Presidencia de la Republica
- **Ley Estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales. - Congreso de la República
- **CONPES 3854 de 2016**: Política Nacional de Seguridad Digital - Consejo nacional de política económica y social – Departamento Nacional de Planeación.
- **Decreto 1083 de 2015**: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. – Presidencia de la República de Colombia.
- **Decreto 1008 de 2018**: Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones. - Presidencia de la República de Colombia.

DOCUMENTOS DE REFERENCIA

A continuación, se detallan los documentos de referencia que se tienen en cuenta para la definición del plan de tratamiento de riesgos de seguridad digital.

- Norma Técnica Colombiana NTC-ISO/IEC 31000:2011 GESTION DEL RIESGO. PRINCIPIOS Y DIRECTRICES
- Norma Técnica Colombiana NTC-ISO 27001:2013 GESTION DE SEGURIDAD DE SISTEMAS DE INFORMACION. PRINCIPIOS Y DIRECTRICES
- Departamento Administrativo de la Función Pública. (2018). Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas. Riesgos de gestion, corrupcion y seguridad digital. Version 4.
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital

LINEAMIENTOS PARA LA DEFINICIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

A continuación, se detallan los lineamientos y pautas a tener en cuenta para la definición del plan de tratamiento de riesgos de seguridad digital.

1. Este debe ser publicado anualmente a más tardar el 31 de enero de cada año y deberá integrarse con los demás planes institucionales y estratégicos de la entidad.
2. Este plan debe definirse con la Oficina Asesora de Planeación y apoyo de la persona encargada de la implementación del sistema de gestión de seguridad de la información.
3. Anualmente se debe definir un cronograma para el plan de tratamiento de riesgos de seguridad digital. Una vez los riesgos sean identificados, clasificados, valorados y tratados, el cronograma puede ser actualizado para realizar la actualización para la gestión de los respectivos riesgos.
4. En el cronograma del plan de tratamiento de riesgos de seguridad digital se debe definir lo siguiente:
    a. Las actividades que se desarrollaran en la vigencia para la cual está definido el plan.
    b. El responsable de la ejecución de cada una de las actividades del plan.
    c. Porcentaje de cumplimiento de cada actividad durante la vigencia.

CRONOGRAMA DE IMPLEMENTACIÓN PLAN DE RIESGOS DE SEGURIDAD DIGITAL

El cronograma de implementación del plan de tratamiento de riesgos de seguridad digital, permite a la entidad definir las actividades necesarias para establecer los controles requeridos para dar el respectivo tratamiento a los riesgos de seguridad digital identificados en cada uno de los procesos de la entidad. Lo anterior con el fin de incrementar los niveles de confidencialidad, integridad y disponibilidad de la información.

Las actividades a desarrollar para la vigencia actual son las siguientes:

1. Identificación de riesgos de seguridad digital en la entidad

1.1 Realizar carga de Activos de información por proceso en el instrumento para la gestión de riesgos de seguridad digital.
1.2 Trasladar riesgos de seguridad y privacidad de la información de la matriz de riesgos de corrupción a la matriz de riesgos de seguridad digital
1.3 Realizar Programación de Entrevistas con Líderes de Procesos
1.4 Realizar entrevistas con Líderes de procesos
1.5 Socializar Política de Administración de Riesgos (Seguridad Digital).
1.6 Socializar Instrumento de Gestión de Riesgos de Seguridad Digital.
1.7 Identificar y clasificar los riesgos de seguridad digital de la entidad

2. Valoración y Tratamiento de Riesgos de Seguridad Digital

2.1 Valorar el Riesgo Residual
2.2 Definir los mapas de calor.
2.3 Ejecutar el plan de tratamiento de riesgos de seguridad digital.
2.4 Realizar seguimiento y control al plan de acuerdo con lo definido en la Guía DAFP

El siguiente es el modelo de Cronograma que se debe establecer anualmente, de acuerdo a lo enunciado en el presente documento.

N°	Nombre Actividad/Tarea	Responsable	2020											
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	**Identificación y Clasificación de riesgos de seguridad digital en la entidad**													
1.1	Realizar carga de activos de información por proceso en el instrumento para la gestión de riesgos de seguridad digital	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información		100%										
1.2	Trasladar riesgos de seguridad y privacidad de la información de la matriz de riesgos de corrupción a la matriz de riesgos de seguridad digital	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información		100%										
1.3	Realizar programación de Entrevistas con Lideres de Procesos	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información		100%										
1.4	Realizar entrevistas con Líderes de procesos	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información		20%	20%	20%	20%	20%						

N°	Nombre Actividad/Tarea	Responsable	2020											
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1.5	Socializar Política de Administración de Riesgos (Seguridad Digital)	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información		20%	20%	20%	20%	20%						
1.6	Socializar Instrumento de Gestión de Riesgos de Seguridad Digital.	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información		20%	20%	20%	20%	20%						
1.7	Identificar y clasificar los riesgos de seguridad digital de la entidad	Oficial de Seguridad de la Información / Oficina Asesora de Planeación / Lideres de proceso		20%	20%	20%	20%	20%						
2	**Valoración y Tratamiento de Riesgos de Seguridad Digital**													
2.1	Valorar el Riesgo Residual	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información				20%	20%	20%	20%	20%				
2.2	Definir los mapas de calor	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información				20%	20%	20%	20%	20%				

N°	Nombre Actividad/Tarea	Responsable	2020											
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
2.3	Ejecutar el plan de tratamiento de riesgos de seguridad digital	Oficina Asesora de Planeación – Lideres de Proceso / apoyo Oficial de Seguridad de la Información								33%	33%	34%		
2.4	Realizar seguimiento y control al plan de acuerdo a lo definido en la Guía DAFP	Oficina Asesora de Planeación / apoyo Oficial de Seguridad de la Información											50%	50%

CONTROL DE CAMBIOS

Control de Cambios		
Fecha	**Versión**	**Descripción**
23/07/2018	1	Creación del documento.
27/01/2020	2	Ajustes generales del documento. Inclusión de los siguientes ítems: documentos de referencia y lineamientos para la definición del plan de riesgos de seguridad digital. Actualización cronograma de implementación plan de tratamiento de riesgos de seguridad digital

Firma de Autorizaciones					
ELABORÓ		**REVISÓ**		**APROBÓ**	
Nombre(s):	Lourdes María Acuña Acuña	**Nombre(s):**	Diego Ferney Ramírez Pulido Pablo Molano Parra	**Nombre(s):**	Andres Javier Solorzano María Ximena De La Cruz
Firma (s):		**Firma (s):**		**Firma (s):**	
Cargo (s):	Contratista TIC	**Cargo (s):**	Contratista TIC Contratista – OAP	**Cargo (s):**	Director de Tecnología y Sistemas de Información Jefe Oficina Asesora de Planeación