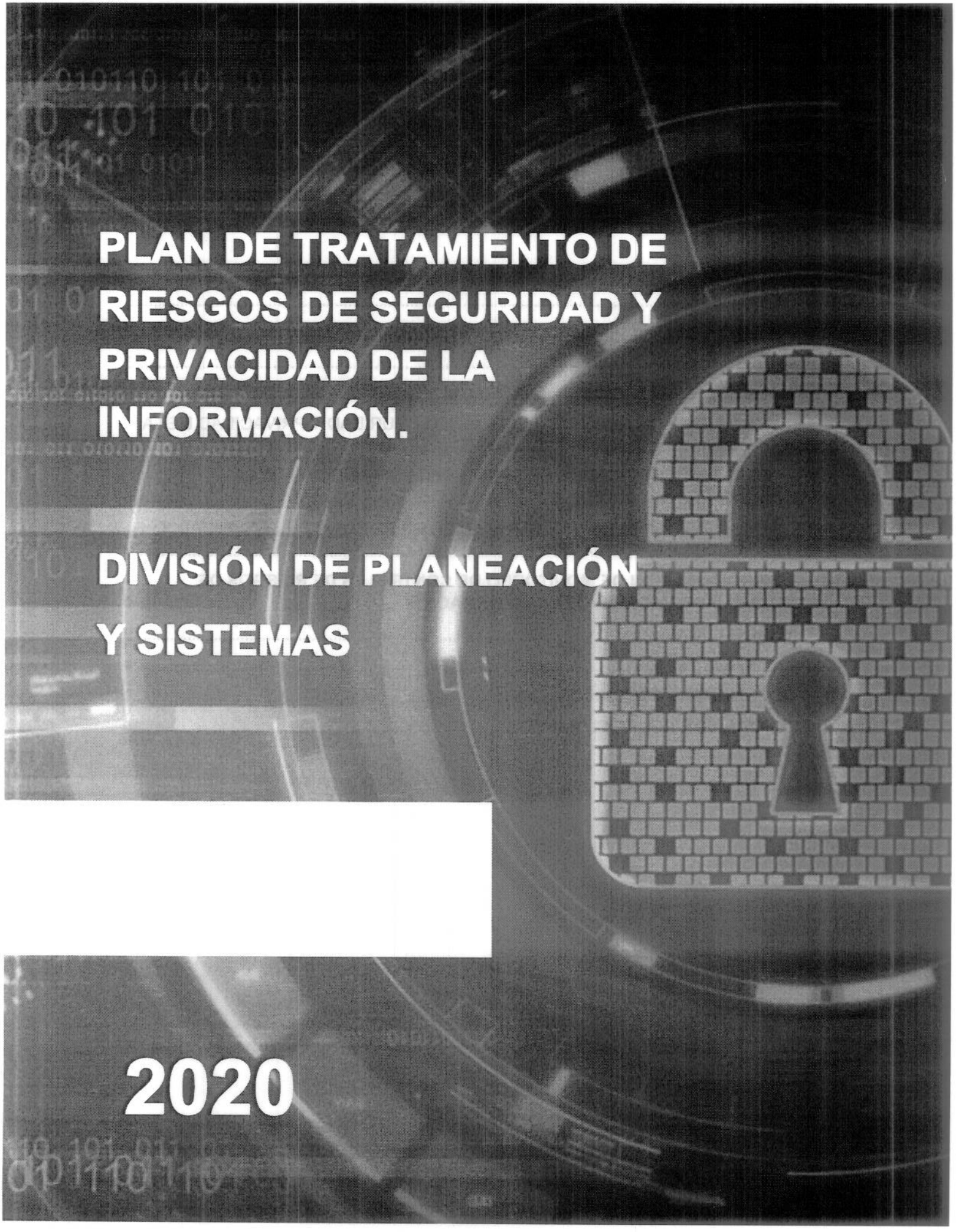


PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

DIVISIÓN DE PLANEACIÓN Y SISTEMAS

2020

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN

El Plan de tratamiento de riesgos de seguridad y privacidad de la información, es una herramienta importante para el Senado de la República, porque permite minimizar perdidas y obtener oportunidades para la protección de los activos de la información de la entidad.

Este plan está orientado a facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión. La información se enmarca en tres principios de protección, que deben ser tenidos en cuenta tanto en la clasificación de los activos, como en el tratamiento de los riesgos de seguridad y privacidad de la información, los cuales son: Confidencialidad, Integridad y Disponibilidad

1. OBJETIVO

Definir un plan de tratamiento de riesgos que precise los controles y acciones necesarias para atenuar la materialización de los riesgos de seguridad de la información en el Senado de la República. De este modo se busca mediante el tratamiento de riesgos fortalecer una adecuada gestión de la información en la entidad.

2. ALCANCE

El plan de tratamiento de riesgos tiene alcance en los activos de información valorados como alto, en el proceso de identificación de riesgos de seguridad digital, de los procesos del Sistema de Gestión de Calidad del Senado de la República.

3. TÉRMINOS Y DEFINICIONES

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: 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.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

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

4. PLANES DESARROLLADOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La identificación de los riesgos de seguridad y privacidad de la información, se realizó teniendo en cuenta la identificación de activos de información, conforme a la guía para realizar el inventario y clasificación de activos de información, los activos de información, que fueron valorados como alto, se les realizó la identificación y valoración de los riesgos.

4.1 RIESGOS IDENTIFICADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RIESGOS	RESPONSABLE DEL CONTROL (Cargo o Sistema)
Pérdida de integridad en el Sistema de nómina.	Asesor II del DPS
Pérdida de confidencialidad en la base de datos del Sistema de asistencia y votación.	Profesional de apoyo del DPS.
Pérdida de disponibilidad en el Sistema de asistencia y votación.	Profesional de apoyo del DPS.
Pérdida de disponibilidad en el Sistema anterior nómina	Asesor II del DPS.
Pérdida de disponibilidad, integridad y confidencialidad de los Servicios virtualizados	Profesionales de apoyo DPS.
Pérdida de Disponibilidad del sistema de gestión de calidad	Profesionales de apoyo DPS.
Pérdida de Disponibilidad del sistema de gestión de Bienes	Profesionales de apoyo DPS.
Falta de Disponibilidad del Profesional Universitario	Jefe de División de Planeación y Sistemas
Pérdida de Disponibilidad del sistema del Firewall e IPS	Profesionales de apoyo DPS.
Pérdida de Disponibilidad del Portal Web	Profesionales de apoyo DPS.
Pérdida de Disponibilidad del servicio de Directorio Activo	Profesionales de apoyo DPS.
Pérdida de Disponibilidad del Servidor de Directorio Activo	Profesionales de apoyo DPS.
Pérdida de Disponibilidad, Confidencialidad e Integridad en el sistema de respaldo	Profesionales de apoyo DPS.
Pérdida de integridad y confidencialidad en el Servidor de gestor documental	Profesionales de apoyo DPS.
Falta de Disponibilidad del Profesional que administra el firewall	jefe de División de Planeación y Sistemas

4.2 ACTIVIDADES A DESARROLLAR SOBRE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (2019 - 2020)

N°	ACCIONES (para enfrentar el riesgo residual)	RESPONSABLE (Ejecución de acciones)	Fecha
1	Realizar la solicitud oportuna de la renovación del contrato de soporte de firewall.	Jefe División de Planeación y Sistemas	31/01/2020
2	Documentar la periodicidad del backup del portal en la nube y local en el formato del procedimiento RT-Pr02 copias de seguridad y restauración de datos para ambientes virtualizados	Profesional de apoyo DPS	30/03/2020
3	Definir la frecuencia en la toma de copias de seguridad, en el formato de backup del procedimiento RT-Pr02 copias de seguridad y restauración de datos para ambientes virtualizados servicio de AD.	Profesionales de apoyo DPS	30/03/2020
4	solicitar para 2020, la adquisición de una herramienta para la administración y gestión del AD	Profesionales de apoyo DPS	30/03/2020
5	Documentar las actividades a realizar para la creación correcta y completa del perfil de usuario del AD, en el RT Pr09 Procedimiento gestión y administración de cuentas institucionales	Profesionales de apoyo DPS	31/01/2020
6	Incluir en la documentación de control de acceso los lineamientos para los usuarios que realizan la publicación en la página web.	Profesional de apoyo DPS	31/01/2020
7	Generar la documentación de lineamientos de control de accesos, que incluya el retiro de usuarios de los grupos creados en el directorio activo.	Profesional Universitario-DPS	31/01/2020
8	Generar tarea de copia de seguridad de la base de datos automáticamente DINAMICA GERENCIAL	Profesional Universitario-DPS	31/01/2020
9	Documentar en las actas de reunión de gestión del cambio, los incidentes evidenciados en el procedimiento de monitoreo.	Profesional de apoyo DPS	31/11/2020
10	Actualizar el documento RT-Pr03 Procedimiento gestión y monitoreo de la plataforma tecnológica	Profesional de apoyo DPS	15/12/2019
11	Incluir en el documento de control de acceso, la segregación de autoridad del responsable de los usuarios de actual gestor documental y el manejo de las cuentas en la aplicación de actual gestor documental	Profesional de apoyo DPS	31/01/2020
12	Incluir actual gestor documental en el plan de continuidad de negocio	Profesional de apoyo DPS	31/01/2020
13	Actualizar el RT-It05 instructivo técnico para contingencia de servicios virtualizados, con alcance a la información técnica del firewall.	Profesional de apoyo-DPS	28/02/2020
14	Generar la documentación de lineamientos de control de accesos, que incluya la restricción de perfiles de accesos de servidores virtualizados.	Profesional de apoyo DPS	15/02/2020
15	Realizar transferencia de conocimiento sobre la administración de firewall, a otro funcionario de la DPS	Profesional de apoyo-DPS	15/02/2020
16	Actualizar el RT-It05 instructivo técnico para contingencia de servicios virtualizados, con alcance al esquema de alta disponibilidad para DARUMA	Profesional Universitario-DPS	28/02/2020
17	Actualizar el RT-It05 instructivo técnico para contingencia de servicios virtualizados, con alcance a la información técnica de los servidores del sistema de gestión de bienes.	Profesional Universitario-DPS	28/02/2020

18	Actualizar el RT-It05 instructivo técnico para contingencia de servicios virtualizados.	Profesional de apoyo DPS	28/02/2020
19	Adquirir una herramienta tecnológica para la toma de copias de seguridad	Profesional de apoyo DPS	31/03/2020
20	Solicitar en 2020, renovación de contrato de soporte oportunamente, para el sistema de nómina de recursos humanos.	Asesor II del DPS, Jefe División Planeación y Sistemas.	30/06/2020
21	Verificar mensualmente las condiciones de los equipos en ambientes de pruebas, para el sistema de recursos humanos. Enviar reporte a Jefe División.	Asesor II del DPS.	31/11/2020
22	Actualizar la documentación del diagrama de red del sistema de asistencia y votación.	Profesionales de Apoyo DPS.	30/03/2020
23	Generar un documento donde se establezca el responsable de aplicar el control, quien tiene acceso a los equipos, la infraestructura de verificación en caso de ser requerido para el sistema DCN	Profesionales de Apoyo DPS.	30/03/2020
24	Documentar la restauración de las copias de seguridad, en el documento Instructivo técnico Rt-It 06 Realización de backups o copias de respaldo y recuperación de desastres informáticos	Profesional de apoyo DPS	28/02/2020
25	Generar los lineamientos documentados para definir la oportunidad de las actualizaciones de antivirus, firewall y sistemas operativos	Profesional de apoyo DPS	30/03/2020
26	Generar ambiente de pruebas, para las actualizaciones de los sistemas operativos y documentarlos en el procedimiento RT-Pr02 copias de seguridad y restauración de datos para ambientes virtualizados	Profesional de apoyo DPS	30/03/2020
27	Realizar transferencia de conocimiento sobre la administración de Dinámica Gerencial, a otro funcionario de la DPS	Profesional Universitario-DPS	30/03/2020
28	Incorporar en el PETI 2020, una actividad de capacitación a los usuarios encargados de publicar en la página web	Profesional de apoyo DPS	30/05/2020
29	Actualizar el RT-It05 instructivo técnico para contingencia de servicios virtualizados con alcance sobre la sincronización del servicio de AD.	Profesionales de apoyo DPS	28/02/2020
30	Generar los lineamientos para la segregación y autoridad del responsable del AD, en el RT Pr09 Procedimiento gestión y administración de cuentas institucionales	Profesionales de apoyo DPS	30 de marzo
33	Definir el anexo técnico, para la renovación de la herramienta de Backup YA	Jefe División Planeación y Sistemas. Profesionales de apoyo DPS	30/03/2020
34	Actualizar el procedimiento RT-Pr02 copias de seguridad y restauración de datos para ambientes virtualizados	Jefe División Planeación y Sistemas. Profesionales de apoyo DPS	30/11/2019

4.3. PROGRAMACIÓN DE MONITOREO DE CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Se realizará una nueva valoración cuando se detecte:

- Nuevos activos o modificaciones en el valor de los activos
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

5. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

6. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

- Norma Técnica Colombiana NTC/ISO 31000 Gestión del Riesgo. Principios y Directrices

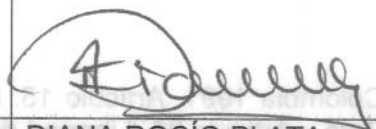
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

7. DOCUMENTOS ASOCIADOS

- RT-Ma02 Manual de Políticas de Seguridad de la Información.
- RT-Ma01- Manual de Políticas de Gestión de Recursos Tecnológicos
- Metodología para el Inventario y la Clasificación de Activos de Información
- Guia para la Administración del Riesgo y Diseño de Controles en Entidades Públicas V.4

8. RESPONSABLE DEL DOCUMENTO

Jefe de la División de planeación y Sistemas.

Proyectó	Revisó	Aprobó
		
Profesionales de apoyo al área de Sistemas	DIANA ROCÍO PLATA ARANGO	ASTRID SALAMANCA RAHÍN
División de Planeación y Sistemas.	Jefe División Planeación y Sistemas.	Directora General Administrativa.