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

SENADO DE LA REPÚBLICA

2023

Contenido

INTRODUCCION

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, de acuerdo con el análisis realizado en la identificación de activos de información.

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

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.

3. MARCO TEORICO

3.1. TERMINOS 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. (Iso 27000.es, 2012).

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. (Iso 27000.es, 2012).

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 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. (Icontec Internacional, 2011).

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada. (Icontec Internacional, 2011).

Control: Medida que modifica el riesgo. (Icontec Internacional, 2011).

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. (Icontec Internacional, 2011).

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. (Icontec Internacional, 2011).

Integridad: Propiedad de la información relativa a su exactitud y completitud. (Iso, 2014).

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. (Icontec Internacional, 2011).

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. (Icontec Internacional, 2011).

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida. (Iso 27000.es, 2012).

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. (Seguridad de la Información TGE, 2016).

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles. (Icontec Internacional, 2011).

Riesgo: Efecto de la incertidumbre sobre los objetivos. (Icontec Internacional, 2011).

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. (Seguridad de la Información TGE, 2016).

SGSI: Sistema de gestión de seguridad de la información (ISO 27000.es, 2012).

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. (Icontec Internacional, 2011).

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.

3.2. SEGURIDAD DE LA INFORMACION

En la actualidad las empresas se enfrentan a muchos riesgos e inseguridades que vienen de diferentes focos, esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades. Según (Instituto Nacional de Ciberseguridad de España, S.A. [INCIBE], 2014) desde tiempos inmemorables las empresas han establecido medidas y técnicas necesarias para evitar y asegurar que los datos no salgan del sistema que ha establecido la organización.

La seguridad de la información busca la creación de una cultura de seguridad en todos los empleados de las empresas y la implementación de controles de seguridad que permitan reducir los riesgos a los que está expuesta y pone en peligro la integridad, confidencialidad y disponibilidad de la información o simplemente ponen a prueba los controles existentes en la empresa y la viabilidad de nuestros negocios.

Es importante reconocer que los riesgos no sólo provienen desde el exterior de cualquier entidad, sino que también pueden estar dentro de la misma, por lo que, para poder trabajar en un entorno de manera segura, se deben tener identificados los activos de información y la fuente de procedencia ya que pueden ser generados por la misma empresa o ser entregados por los clientes y estar en diferentes medios, como físicos y digital. Por lo anterior la empresa se puede apoyar en la implementación un sistema de Gestión de seguridad de la información – SGSI que permita asegurar la información y disponer de controles que permita disminuir el impacto de los riesgos.

Cabe resaltar la diferenciar entre seguridad informática y seguridad de la información:

La primera, se refiere a la protección de la infraestructura de las tecnologías de la información y comunicación que soportan la empresa, mientras que la seguridad de la información se refiere a la protección de los activos de información fundamentales para el éxito de cualquier organización que soportan la organización (INCIBE, 2014).

En el ítem 3.1 Términos y definiciones, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo del plan de riesgos, relacionado con la gestión del riesgo y la seguridad de la información.

A continuación, se presentan las definiciones desde los puntos de vista de seguridad de la información y de riesgos, la cual está alineada a la definición de la norma:

- **Confidencialidad:** Es garantizar el acceso a la información sólo a los usuarios autorizados" (Seguridad de la Información de TGE, 2016). A nivel de riesgos: "la información es accesible solamente a quienes están autorizados para ello. Información cuya divulgación puede generar desventajas competitivas, pérdidas económicas, afecta la reputación y/o imagen y de la compañía" (Seguridad de la Información TGE, 2016).

- **Integridad:** "Evitar que la información sea modificada de manera no autorizada" (Seguridad de la Información de TGE, 2016). A nivel de riesgos: "Protección de la exactitud y estado completo de la información y métodos de procesamiento. Información sin errores ni fraude, la ocurrencia de alguna de estas ocasionará pérdidas significativas" (Seguridad de la Información TGE, 2016).

- **Disponibilidad:** “Garantizar que la información esté disponible cuando se necesite” (Seguridad de la Información de TGE, 2016). “A nivel de riesgos: Seguridad que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren. La información debe ser accesible y recuperable fácilmente en caso de suspensión del procesamiento” (Seguridad de la Información TGE, 2016).

3.2.1. NORMA ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Norma constituye también los requisitos para la valoración y el tratamiento de los riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicados a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (ICONTEC Internacional, 2013). Podemos definir un Sistema de Gestión de Seguridad de la Información como una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información (confidencialidad, integridad y disponibilidad) de la organización (INCIBE, 2014) La implementación de la Norma permite establecer políticas, procedimientos y controles con el objeto de mitigar o eliminar los riesgos de su organización, para lograrlo la entidad ha considerado implementar y mantener el SGSI, involucrando:

- Definición de políticas, estándares, procedimientos y formatos.
- Gestión de riesgos de seguridad de la información sobre los procesos de la entidad del SGSI que involucran los activos de información. La cual se basa en el análisis, evaluación y tratamiento de estos de acuerdo con el estándar ISO/IEC 31000.
- Cumplimiento de obligaciones legales, regulatorias y contractuales relacionadas con Seguridad de la Información.
- Gestión de incidentes de Seguridad de la Información. • Entrenamiento y sensibilización en seguridad de la información” (Seguridad de la Información de TGE, 2016).

3.2.2. NORMA ISO/IEC 27002:2013 Código para la práctica de la gestión de la seguridad de la información

Norma internacional que establece el código de las mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI), Junto a los controles a implementar de acuerdo con la empresa al momento de hacer la valoración y definición del plan de tratamiento de riesgos de seguridad de la información.

Está norma compuesta por 14 dominios, es decir áreas de actuación, 35 objetivos de control o aspectos a asegurar dentro de cada área y 114 controles o mecanismos para asegurar los distintos objetivos de control, que se encuentran definidas en el modelo de seguridad y privacidad de la información del Senado, a través de la declaración de aplicabilidad

3.2.3. NORMA ISO 31000:2009 Gestión de Riesgos

La Norma ISO 3100 es un estándar para la gestión de riesgos, que al igual que la ISO 27001 para el sistema de gestión de seguridad de la información, puede ser implementado en: Organizaciones de todo tipo y tamaños, sin importar el objeto de negocio, los procesos y sus niveles, debido a que cualquiera puede enfrentar factores internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el "riesgo" (Icontec, 2011).

La ISO 31000 enumera los principios para una gestión eficaz del riesgo. El fin de estos principios es el de conformar y reorientar los aspectos del enfoque de la organización u empresa a la gestión del riesgo, dichos principios describen las características de una gestión eficaz del riesgo.

Es importante que las organizaciones conozcan, detallen y reflejen todos los aspectos de la gestión, para ello tendrán que diseñar indicadores de desempeño de la gestión del riesgo, y reforzar el valor que tiene para la organización, el hecho de tener que gestionar el riesgo de una manera eficaz y sobre todo profesional. La ISO 31000 identifica elementos de un marco de trabajo de gestión del riesgo en donde existen ventajas que se muestran cuando los elementos de todo ese trabajo están integrados en la alta dirección de la organización o empresa, así como en sus funciones y procesos.

En el plan de tratamiento de riesgos de seguridad y privacidad de la información para el senado de la Republica se tendrá en cuenta esta Norma como guía, en conjunto con la guía para la gestión de riesgo de la función pública, siguiendo sus recomendaciones y directrices para realizar una eficaz y eficiente gestión de riesgos de seguridad de la información.

3.2.4. TRATAMIENTO DE RIESGOS

El tratamiento de riesgos permite seleccionar e implementar opciones para abordar el riesgo. "El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica" (Icontec, 2011).

El tratamiento del riesgo implica un proceso repetitivo de:

- Formular y seleccionar opciones para el tratamiento del riesgo
- Planificar e implementar el tratamiento del riesgo
- Evaluar la eficacia de ese tratamiento
- Decidir si el riesgo residual es aceptable
- Si no es aceptable, efectuar tratamiento adicional.

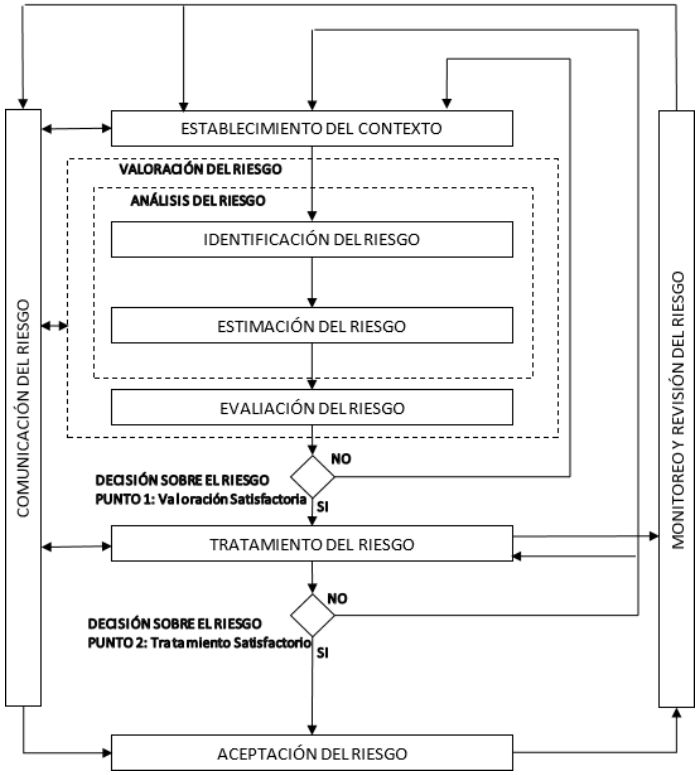


Ilustración 2. Proceso para la administración de riesgos de seguridad y privacidad de la información Fuente: https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf

En el marco del Modelo de Seguridad y Privacidad de la Información del Senado de la República, se busca prevenir los efectos no deseados o no esperados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y definir los riesgos de seguridad de la información. De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo.

A partir del inventario de activos de información con el que cuenta el Senado de la Republica; se realizó una clasificación de acuerdo con el Manual de Gestión del Riesgo del Departamento Administrativo de la Función Pública (DAFP) que establece tres pilares o principios de la Seguridad de la Información: Confidencialidad, integridad, disponibilidad. Los activos de información, que fueron valorados como alto, se les realizó la identificación y valoración de los riesgos.

A continuación, se presentan la representación para la clasificación de los riesgos, de acuerdo con la integridad, confidencialidad y disponibilidad, desde los puntos de vista de seguridad de la información y de riesgos, la cual está alineada a la definición de la norma:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

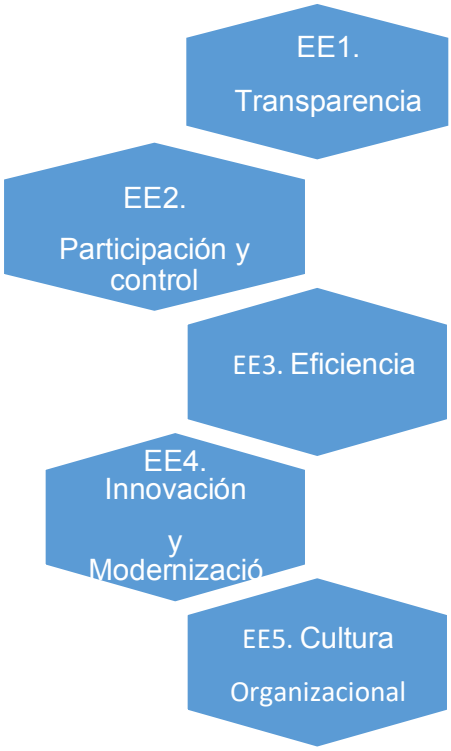
Tabla1. Criterios de clasificación
https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla2. Niveles de clasificación
https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

4. ESTRATEGIAS

Dentro del plan estratégico 2021 -2024 del Senado de la Republica se encuentran los siguientes 5 ejes estratégicos: Transparencia, participación y control ciudadano, eficiencia, Innovación y Modernización Tecnológica y Cultura organizacional.



Dentro del eje estratégico 4 Innovación y modernización tecnológica, se encuentran considerada la estrategia 4.1 Continuar con la modernización de la infraestructura tecnológica, que incorporan dos iniciativas para los temas de seguridad y privacidad de la información, y evidencian la alineación del plan con el plan estratégico de acuerdo con lo definido en el Decreto 612 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.”

Iniciativas

* Elaborar y ejecutar el Plan de tratamiento de riesgos de Seguridad y privacidad de la Información.

Con esta se busca fortalecer la seguridad de la información y seguridad digital en el Senado de la República y prevenir la consolidación de riesgos y fortalecer los controles asociados.

5. PLAN DESARROLLADO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El proceso de gestión de riesgo en la seguridad de la información manifiesta la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

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, teniendo en cuenta la guía de la función pública para la gestión del riesgo.

5.1. RIESGOS IDENTIFICADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACION

No DE RIESGO	DESCRIPCIÓN DEL RIESGO
R1	Pérdida de disponibilidad en el sistema de nómina Software Kactus.
R2	Pérdida de confidencialidad en la base de datos del sistema de asistencia y votación de plenaria.
R3	Pérdida de disponibilidad en el sistema de asistencia y votación de plenaria.
R4	Probabilidad de afectación por pérdida de disponibilidad en el sistema Hominis.
R5	Pérdida de disponibilidad de los servicios VIRTUALIZACIÓN HYPER-V.
R6	Pérdida de integridad de los servicios de VIRTUALIZACIÓN HYPER-V.
R7	Pérdida de confidencialidad de los servicios de VIRTUALIZACIÓN HYPER-V.
R8	Pérdida de disponibilidad del sistema de gestión de calidad DARUMA.
R9	Pérdida de disponibilidad del sistema de gestión de Bienes DINÁMICA GERENCIAL.
R10	Pérdida de disponibilidad, integridad y confidencialidad del sistema del Firewall.
R11	Pérdida de disponibilidad, integridad y confidencialidad del IPS.
R12	Pérdida de disponibilidad del portal Web.
R13	Pérdida de disponibilidad del servicio de Directorio Activo.
R14	Pérdida de disponibilidad del servidor de Directorio Activo.
R15	Posibilidad de afectación económica por multa de la Superintendencia de Industria y Comercio, debido a tratamiento de datos personales sin la autorización expresa del titular.

R16	Posibilidad de afectación reputacional por demanda o queja del titular de los datos, por el uso indebido de las grabaciones de cámaras de vigilancia de seguridad.
R17	Posible afectación reputacional por falta de disponibilidad e integridad de los servidores alojados en la nube privada, debido a falla en el enlace de conexión.
R18	Posibilidad de afectación reputacional, por la pérdida de disponibilidad del servicio, debido a la falta de renovación del licenciamiento y soporte técnico del WAF.
R19	Posible afectación económica y reputacional por perdida de información, debido a presencia de malware o ransomware en la plataforma tecnológica de la Entidad.
R20	Posible afectación económica y reputacional por Acceso a la red o al sistema de información generando suplantación de sitio web debido a conexiones a red pública desprotegidas
R21	Posible afectación reputacional por error en la publicación de los conjuntos de datos abiertos debido a entrenamiento deficiente y falta validación de calidad de los datos.

5.2. ACTIVIDADES PARA DESARROLLAR SOBRE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (2022 - 2023)

No DE RIESGO	PLAN DE ACCIÓN	RESPONSABLE
R1	Documentar en las actas de gestión de cambios, las actualizaciones de versión de cada uno de los sistemas de información. FV: Actas de gestión de Cambios	Asesor II – División Planeación y Sistemas.
R2	Documentar las actividades correspondientes a verificación de permisos de acceso al sistema de plenaria en el Procedimiento RT-Pr09 Gestión y administración de Cuentas. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.
R3	Presentar ante la DGA, documentación para la contratación de la mesa de servicios. FV: Documentación presentada.	Profesional Universitario – División Planeación y Sistemas.
R5	Presentar ante la DGA, documentación para la contratación de la mesa de servicios. FV: Documentación presentada.	Profesional Universitario – División Planeación y Sistemas.
R5	Mantener actualizado el Catálogo de sistemas de información, con el registro de las últimas versiones liberadas. FV: Catalogo de sistemas de información actualizado.	Asesor II – División Planeación y Sistemas.
R5	Mantener actualizado el Catálogo de sistemas de información, con el registro de las últimas versiones liberadas. FV: Catalogo de sistemas de información actualizado.	Asesor II – División Planeación y Sistemas.
R5	Analizar el resultado del reporte de monitoreo, generado por el sistema Orión. FV: Acta Gestión de Cambio y reporte.	Asesor II – División Planeación y Sistemas.

R5	Analizar el resultado del reporte de monitoreo, generado por el sistema Orión. FV: Acta Gestión de Cambio y reporte.	Asesor II – División Planeación y Sistemas.
R5	Analizar el resultado del reporte de monitoreo, generado por el sistema Orión. FV: Acta Gestión de Cambio y reporte.	Asesor II – División Planeación y Sistemas.
R6	Presentar solicitud ante la DGA, para la adquisición de herramienta de análisis de vulnerabilidades para los dispositivos de hardware y software de la Entidad. FV: Solicitud presentada ante la DGA.	Asesor II – División Planeación y Sistemas.
R6	Actualizar el Procedimiento RT-Pr04 Control de Cambios, para incluir la información mínima que se registra en las actas de Control de Cambios. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.
R6	Actualizar el Procedimiento RT-Pr09 Gestión y administración de cuentas institucionales, para incluir el reporte de perfiles de Directorio Activo. FV: Documento aprobado.	Asesor II – División Planeación y Sistemas.
R7	Realizar validación mensual de las amenazas del boletín de ciberseguridad generado por el CSIRT de Gobierno. FV: Acta de gestión de cambios.	Asesor II – División Planeación y Sistemas.
R7	Mantener actualizado el Catálogo de sistemas de información, con el registro de las últimas versiones liberadas. FV: Catalogo de sistemas de información actualizado	Asesor II – División Planeación y Sistemas.
R8	Documentar el control No. 1, dentro del Procedimiento RT-Pr01 Soporte técnico y atención de servicios, para incluir la solicitud de mantener el contrato de Soporte con el fabricante del software, con el fin de garantizar el soporte del sistema de información. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.
R11	Documentar el control No. 2, dentro del Procedimiento RT-Pr01Soporte técnico y atención de servicios, para incluir la solicitud de mantener el contrato de Soporte y renovación de licenciamiento con el fabricante del software, con el fin de garantizar el soporte de la solución FW. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.
R12	Solicitar renovación de la herramienta de seguridad, tipo WAF para mejorar la capacidad de respuesta ante ataques informáticos. FV: comunicación Interna con anexo técnico a DGA.	Profesional Universitario – División Planeación y Sistemas.
R12	Solicitar la actualización del alojamiento de la página web, con características que pueda garantizar un nivel de seguridad más alto frente a ataques informáticos. FV: comunicación Interna a la DGA.	Asesor II – División Planeación y Sistemas.

R12	Mantener un servidor local de respaldo, con el fin de garantizar la continuidad del servicio. FV: Acta de control de Cambios.	Asesor II – División Planeación y Sistemas.
R12	Actualizar el Procedimiento RT-Pr04 Control de Cambios, para incluir la información mínima que se registra en las actas de Control de Cambios. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.
R13	Solicitar una solución informática para la actualización del directorio activo. Fv: Comunicación enviada a DGA con el anexo técnico.	Asesor II – División Planeación y Sistemas.
R15	Enviar piezas informativas a los funcionarios y contratistas de la Entidad, con el fin de sensibilizar acerca de la importancia del uso adecuado de los datos personales. FV: Registro de las comunicaciones.	Asesor II – División Planeación y Sistemas.
R15	Enviar piezas informativas a los funcionarios y contratistas de la Entidad, con el fin de sensibilizar acerca de la importancia del uso adecuado de los datos personales. FV: Registro de las comunicaciones.	Asesor II – División Planeación y Sistemas.
R15	Actualizar el Formato PC-Fr09Lista de chequeo para contratación directa de persona natural. FV: Documento aprobado.	Asesor II – División Planeación y Sistemas.
R16	Actualizar el formato RT-Fr01Solicitud de registros y grabaciones de seguridad. FV: Documento aprobado.	Asesor II – División Planeación y Sistemas.
R19	Realizar divulgación a los usuarios acerca de la importancia de no descargar información de correo sospechoso. FV: Registro de la divulgación.	Asesor II – División Planeación y Sistemas.
R20	Documentar en instructivo técnico configuración del WAF. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.
R20	Solicitar a DGA renovación de hosting con condiciones seguras. FV: Solicitud dirigida a DGA.	Profesional Universitario – División Planeación y Sistemas.
R21	Actualizar instructivo RT-It37 con la información de como validar la calidad de los datos. FV: Documento aprobado.	Profesional Universitario – División Planeación y Sistemas.

Para la vigencia 2023 se priorizan los siguientes factores de riesgo digital en el plan de tratamiento de riesgos:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura
- Identificación y protección de los datos de carácter personal

- Adecuada clasificación de la información bajo custodia de la Entidad de acuerdo con el marco legal vigente
- Entorno global digital inseguro
- Segregación apropiada de roles y privilegios en todos los sistemas de información
- Acceso seguro a la red en todas las sedes de la entidad

5.3. PROGRAMACIÓN DE MONITOREO DE CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD 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.

5.4. MEDICIÓN AL SISTEMA DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente en la medición de eficacia de todos los componentes de implementación y gestión que se encuentran definidos en el modelo de operación del marco de seguridad y privacidad de la información MSPI, este indicador se alimenta de indicadores internos lo que permite medir la efectividad, eficacia y eficiencia de la seguridad de la información dentro de la entidad y cuyos resultados servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la información. Los indicadores propuestos se encuentran en la guía N-9 de indicadores de gestión para la seguridad de la información MinTIC.

6. 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.

6.1. NORMATIVA VIGENTE

NORMA	AÑO	EPIGRAFE	ARTICULO(S)
LEY ESTATUTARIA 1581	2012	disposiciones generales para la protección de datos personales	Toda la norma
Ley 1341	2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea laAgencia Nacional de Espectro y se dictan otras disposiciones	Toda la norma
CONPES 3701	2011	Lineamientos de política para ciberseguridad y ciberdefensa.	Toda la norma
CONPES 3854	2017	Política nacional de seguridad digital	Toda la norma
CONPES 3920	2018	Política nacional de explotación de datos (BIG DATA)	Toda la norma
CONPES 3995	2020	Política nacional de confianza y seguridad digital	Toda la norma
Decreto 1078	2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones	Toda la norma
Decreto 1081	2015	Decreto Reglamentario Único del Sector Presidencia de la República (ultima actualización 25 de nov de 2021)	Libro 2
Decreto 415	2016	Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.	Toda la norma
Decreto 1499	2017	modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.	Capítulo 2
Decreto 1413	2017		

Resolución CDS 004	2017	Fortalecimiento Institucional en materia de TIC, Plan estratégico de tecnología y sistemas de información (PETI) y para la gestión de proyectos TIC	Toda la norma

Nota: Información actualizada del documento publicado de la secretaria distrital de gobierno pagina 5 y 6 "Plan de tratamiento de riesgos de seguridad y privacidad de la información".

7. REQUISITOS TÉCNICOS

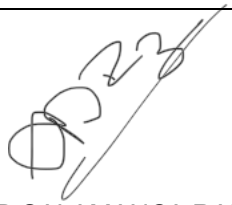
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de laseguridad de la información.
- Norma Técnica Colombiana NTC/ISO 31000 Gestión del Riesgo. Principios yDirectrices
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologíasy Sistemas de Información.

8. 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
- Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas V.5

9. RESPONSABLE DEL DOCUMENTO

Jefe de la Division de Planeación y Sistemas

ELABORÓ	REVISÓ	APROBÓ
Profesionales de apoyo al área de sistemas	 PABLO EDUARDO ALZATE PEREZ	 ASTRID SALAMANCA RAHIN
División Planeación y Sistemas.	jefe División Planeación y Sistemas(E)	Directora General Administrativa