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

SENADO DE LA REPÚBLICA

2025

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 de Tratamiento de Riesgos de Seguridad y privacidad de la Información representa un compromiso sólido con la protección y preservación de la integridad de la información sensible que maneja esta honorable institución. Ante las crecientes amenazas cibernéticas, esta propuesta establece un marco estratégico para identificar, evaluar y mitigar riesgos, asegurando la confidencialidad y disponibilidad de la información vital para el funcionamiento transparente y eficiente de nuestro Senado.

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.

El plan de tratamiento de Riesgos tendrá en cuenta los riesgos que se encuentren en nivel alto, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la entidad.

3. MARCO TEÓRICO

3.1. 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. (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).

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.

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 de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

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).

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

3.2. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se refiere a la protección de la información contra amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad. Este concepto abarca un amplio espectro de medidas y prácticas diseñadas para garantizar que la información sensible esté resguardada de accesos no autorizados, modificaciones no deseadas y pérdidas o indisponibilidades no planificadas.

Algunos aspectos clave de la seguridad de la información incluyen:

- **Confidencialidad:** Garantizar que la información solo esté disponible para aquellos que tienen los permisos necesarios para acceder a ella.
- **Integridad:** Asegurar que la información no sea alterada de manera no autorizada o accidental y que permanezca exacta y completa.
- **Disponibilidad:** Asegurar que la información esté disponible cuando sea necesario y que los sistemas que la procesan estén operativos.
- **Autenticación:** Verificar la identidad de usuarios y sistemas para asegurarse de que solo aquellos autorizados tengan acceso.
- **Autorización:** Definir y gestionar los permisos y derechos de acceso para garantizar que los usuarios solo tengan acceso a la información que necesitan para realizar sus funciones.
- **Respaldo y recuperación:** Implementar procedimientos para respaldar regularmente la información crítica y establecer planes de recuperación ante desastres para minimizar el impacto en caso de incidentes.
- **Cifrado:** Utilizar técnicas de cifrado para proteger la información durante su transmisión y almacenamiento, de modo que incluso si un tercero no autorizado accede a ella, no pueda comprenderla.
- **Concientización:** Educar a los usuarios y al personal sobre las mejores prácticas de seguridad, promoviendo una cultura de conciencia y responsabilidad en relación con la información.
- **Monitoreo y auditoría:** Implementar sistemas de monitoreo continuo y auditorías regulares para detectar y responder a actividades sospechosas o violaciones de seguridad.
- **Gestión de riesgos:** Evaluar y gestionar proactivamente los riesgos potenciales para la seguridad de la información, implementando medidas preventivas y correctivas.

La seguridad de la información es esencial en el mundo digital actual, donde la información se comparte y almacena en diversas plataformas y sistemas. La implementación efectiva de medidas de seguridad ayuda a proteger la privacidad, la confidencialidad y la integridad de la información, así como a garantizar la continuidad de las operaciones empresariales.

Así mismo, 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.

3.2.1. NORMA ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad.

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 evaluación 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, 2022).

Se puede definir un Sistema de Gestión de Seguridad de la Información (SGSI), como un marco integral y sistemático que establece políticas, procedimientos y procesos para gestionar, controlar y mejorar la seguridad de la información dentro de una organización. El objetivo principal de un SGSI es proteger la confidencialidad, integridad y disponibilidad de la información frente a amenazas internas y externas.

Para lograrlo la entidad ha considerado implementar y mantener el SGSI, involucrando:

- Definición de Política de Seguridad de la Información:
- Análisis de Riesgos:
- Controles de Seguridad:
- Gestión de Activos de Información:
- Acceso Lógico y Físico:
- Concientización y Formación:
- Gestión de Incidentes:
- Monitoreo y Medición:
- Revisión por la Dirección:
- Mejora Continua:

La implementación de un SGSI, particularmente bajo estándares como ISO/IEC 27001, puede ayudar a las organizaciones a demostrar el compromiso con la seguridad de la información y a cumplir con requisitos legales y regulatorios. Además, proporciona un marco estructurado para abordar los desafíos constantes relacionados con la seguridad en el entorno digital.

3.2.2. NORMA ISO/IEC 27002:2022 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 principales, es decir áreas de actuación, y 93 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 31000:2018 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.

3.3. POLITICA DE ADMINISTRACION DE RIESGOS

El Senado de la República, establece los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios, procurando que no se materialicen, atendiendo los lineamientos establecidos en la guía para la

administración del riesgo y el diseño de controles en entidades públicas del DAFP[1], orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los grupos de interés.

3.3.1. 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.

1 ~~https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf~~https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

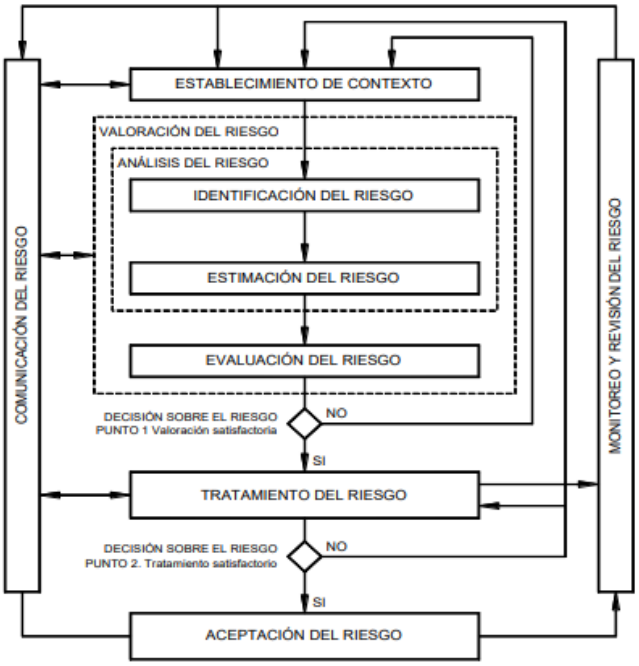

Ilustración 1. Proceso para la administración de riesgos de acuerdo con ISO 27005

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 República; 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

Ilustración 2. Criterios de clasificación

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.

Ilustración 3. Niveles de clasificación

El resultado de esta valoración se refleja en el RT-Fr10 formato inventario, valoración y clasificación de activos de información, a partir del cual se seleccionan para tratamiento de riesgos, los activos de información clasificados con nivel de criticidad alta.

4. ESTRATEGIAS

Dentro del plan estratégico 2025 -2028 del Senado de la Republica se encuentran los siguientes 5 ejes estratégicos: Transparencia y rendición de cuentas, participación ciudadana y calidad del servicio, cultura organizacional, gestión del conocimiento y la innovación y eficiencia y productividad.

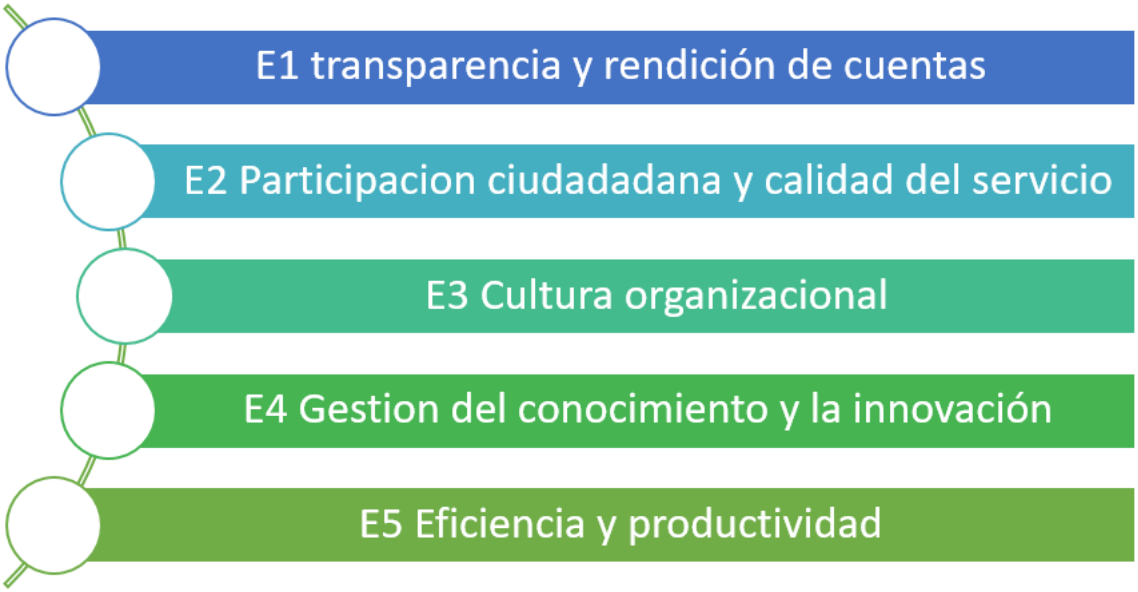

Ilustración 4. Alineación plan estratégico

Dentro del eje estratégico 5 Eficiencia y productividad, se encuentran considerado el objetivo estratégico OE9 Continuar con la modernización de la infraestructura tecnológica, y evidencian la alineación con el plan estratégico de acuerdo con lo definido en el Decreto 612 de 2018.

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.

Activos de Información Procesos SGSI
Resumen de Activos

Criticidad del Activo	Cantidad de Activos
Alto	1
Moderado	2
Bajo	6
Total	**9**

Ilustración 2: Identificación de Activos de información

5.1. RIESGOS IDENTIFICADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

No DE RIESGO	DESCRIPCIÓN DEL RIESGO
R1	Pérdida de disponibilidad en el sistema de nómina Software Kactus.
R2	Pérdida de integridad en el servidor que aloja el Sistema de nómina Software Kactus.
R3	Probabilidad de afectación por Pérdida de disponibilidad en el Sistema Hominis
R4	Pérdida de disponibilidad de los Servicios HYPERCONVERGENCIA
R5	Pérdida de integridad de los Servicios de HYPERCONVERGENCIA
R6	Pérdida de Confidencialidad del sistema de gestión documental CONTROLDOC
R7	Pérdida de Disponibilidad y confidencialidad del sistema del Firewall
R8	Pérdida de Disponibilidad, integridad y confidencialidad del IPS
R9	Pérdida de Confidencialidad del Portal Web
R10	Pérdida de Integridad del Portal Web
R11	Pérdida de Disponibilidad del Portal Web
R12	Pérdida de Integridad del Servidor de Directorio Activo
R13	Pérdida de Disponibilidad del Servidor de Directorio Activo.
R14	Posibilidad de afectación económica por multa de la Superintendencia de Industria y Comercio, y/o sanción disciplinaria por parte de la Procuraduría General de la Nación, debido a tratamiento de datos personales sin la autorización expresa del titular.
R15	Perdida de Disponibilidad del sistema Powerfile.
R16	Perdida de Confidencialidad del Sistema Powerfile

Para la vigencia 2025 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
- Segmentación y Acceso seguro a la red en todas las sedes de la entidad

5.2. DEFINICIÓN DE MAPA DE RIESGOS Y PLANES DE TRATAMIENTO

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, los líderes de los procesos deben realizar la aprobación de los mapas de riesgos y planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual se encuentre en zona Alta.

5.3. MATERIALIZACIÓN

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con formato informe análisis de gestión del riesgo y efectividad de los controles.

Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

5.4. MONITOREO

Se realizará una nueva valoración cuando se detecte:

- Nuevos activos o modificaciones en el valor de los activos
- Cambios en el contexto interno o externo.

- 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.

5.5. MEDICIÓN

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[2].

ELABORÓ	REVISÓ	Aprobado mediante Acta Nro.25-01 27 de Enero-2025 Comité Institucional de Gestión y Desempeño
Juan Carlos Ramos S. 	Lenin José Palomino Blanco 	ASTRID SALAMANCA RAHIN
Asesor 2 División Planeación y Sistemas	Jefe División Planeación y Sistemas	Directora General Administrativa

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf