E.S.E.
RAFAEL TOVAR POVEDA
NIT. 900211477-1

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

TABLA DE CONTENIDO

1. OBJETIVOS

OBJETIVO GENERAL

Garantizar que los directivos, funcionarios, contratistas y demás usuarios de la E.S.E. RAFAEL TOVAR POVEDA gestionen de manera sistemática, oportuna y documentada los riesgos de seguridad y privacidad de la información, mediante la aplicación del Plan de Tratamiento de Riesgos descrito en este documento, alineado con el Sistema de Gestión de Seguridad de la Información (SGSI), la NORMA ISO/IEC 27001:2022 y la normatividad vigente, con el fin de mantener la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

OBJETIVOS ESPECIFICOS

- Identificar y mantener actualizados los riesgos de seguridad y privacidad de la información asociados a los procesos, activos de información y servicios de la E.S.E. RAFAEL TOVAR POVEDA, utilizando una metodología institucional definida y documentada.
- Valorar la probabilidad y el impacto de los riesgos identificados, determinando su nivel de riesgo y priorizando aquellos que requieran tratamiento, de acuerdo con los criterios establecidos por la institución.
- Definir, documentar y mantener actualizado un Plan de Tratamiento de Riesgos de seguridad y privacidad de la información, que especifique las opciones de tratamiento seleccionadas (evitar, mitigar, transferir o aceptar), los controles propuestos, los responsables y los plazos de implementación.
- Integrar las acciones de tratamiento de riesgos de seguridad y privacidad de la información en los planes, procedimientos y controles operativos de la E.S.E., articulándolas con el Plan de Seguridad y Privacidad de la Información, el SGSI y el Sistema de Gestión de la Calidad institucional.
- Establecer mecanismos de seguimiento, medición e informe sobre el estado de los riesgos y de las acciones de tratamiento, que permitan evaluar la eficacia de los controles implementados, tomar decisiones informadas y evidenciar la trazabilidad de las decisiones ante la Alta Dirección y los entes de control.
- Promover en los directivos, funcionarios, contratistas y terceros una cultura de gestión de riesgos de seguridad y privacidad de la información, que fortalezca el cumplimiento de las políticas institucionales, la normatividad aplicable y los principios de confidencialidad, integridad, disponibilidad y privacidad de los datos.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. RAFAEL TOVAR POVEDA aplica a todos los procesos, dependencias, sedes y usuarios que manejen, procesen, transmitan, almacenen o administren información institucional, independientemente del medio o soporte en el que ésta se encuentre (físico, digital, audiovisual, etc.).

Desde:

- Todos los directivos, funcionarios, contratistas, prestadores de servicios y terceros que, en el desarrollo de sus funciones o relaciones contractuales, tengan acceso a información institucional o a los sistemas y recursos tecnológicos de la E.S.E.
- Todos los activos de información relacionados con la gestión misional, administrativa, financiera, asistencial, estadística, de calidad, gestión documental y demás áreas de la E.S.E., incluyendo datos personales y datos sensibles, tales como la historia clínica y demás información de los usuarios de los servicios de salud.
- A los servicios, plataformas, soluciones tecnológicas y proveedores externos que procesen, almacenen, transmitan o tengan acceso a información institucional o de los usuarios, incluyendo esquemas de interoperabilidad, servicios en la nube, soporte tecnológico, mantenimiento de sistemas y terceros que actúen como encargados del tratamiento de datos personales, en los términos establecidos por la normatividad vigente.

Hasta:

La identificación, análisis, valoración, priorización y tratamiento de los riesgos de seguridad y privacidad de la información asociados a:

- Procesos misionales, de apoyo y estratégicos de la E.S.E.
- Activos de información (información, aplicaciones, bases de datos, infraestructuras tecnológicas, medios de almacenamiento, equipos, archivos físicos, etc.).
- Uso de redes, sistemas de información, aplicaciones clínicas y administrativas, servicios en línea y canales de comunicación internos y externos.

El presente Plan:

- Cubre las actividades de identificación, valoración, definición de opciones de tratamiento, selección de controles, elaboración del Plan de Tratamiento de Riesgos, seguimiento y actualización de los riesgos de seguridad y privacidad de la información.

- Se articula con el Plan de Seguridad y Privacidad de la Información, el Sistema de Gestión de Seguridad de la Información (SGSI), el Sistema de Gestión de la Calidad y el Modelo Integrado de Planeación y Gestión (MIPG) adoptado por la E.S.E.
- Aplica a todas las sedes, puntos de atención y servicios institucionales que generen, reciban, consulten o custodian información de la E.S.E. o de los usuarios de los servicios de salud.

No hace parte del alcance de este Plan la gestión detallada de riesgos clínicos, financieros, laborales o de otro tipo que no tengan relación directa con la seguridad y privacidad de la información; sin embargo, cuando estos riesgos se encuentren relacionados con el uso o tratamiento de información, se deberán articular con la gestión de riesgos de seguridad de la información definida en este documento.

3. NORMATIVIDAD

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. RAFAEL TOVAR POVEDA se fundamenta, entre otros, en los siguientes referentes normativos y técnicos (susceptibles de actualización según cambios posteriores en la regulación nacional o en los estándares internacionales aplicables):

Constitución Política de Colombia: artículos 15, 20 y concordantes, relacionados con el derecho a la intimidad, el hábeas data y el acceso a la información.

Ley 1581 de 2012 y sus decretos reglamentarios: por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1266 de 2008: por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, especialmente en lo relacionado con riesgo financiero y crediticio.

Ley 1273 de 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado (la protección de la información y de los datos) y se tipifican los delitos informáticos.

Ley 594 de 2000 – Ley General de Archivos y normas reglamentarias expedidas por el Archivo General de la Nación, en lo referente a la gestión documental, conservación, custodia y disposición de documentos físicos y electrónicos.

Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y sus decretos reglamentarios, en lo relacionado con la gestión, publicación y acceso a la información pública.

Normatividad del sector salud aplicable a la historia clínica y a la protección de la información del paciente, incluyendo resoluciones, circulares y lineamientos vigentes del Ministerio de Salud y Protección Social y de la Superintendencia Nacional de Salud.

Modelo Integrado de Planeación y Gestión – MIPG y lineamientos del Departamento Administrativo de la Función Pública, especialmente en lo relacionado con gestión del riesgo, seguridad digital y gestión de la información.

Guías y lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) sobre tratamiento de riesgos de seguridad y privacidad de la información, seguridad y privacidad digital y gestión de incidentes de seguridad de la información en entidades públicas.

ISO/IEC 27001:2022 – Tecnología de la información – Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información, como estándar de referencia para la gestión de riesgos de seguridad de la información y el establecimiento del SGSI.

ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información, como guía para la selección de controles asociados al tratamiento de riesgos.

ISO/IEC 27005 (versión vigente) – Tecnología de la información – Técnicas de seguridad – Gestión de riesgos de seguridad de la información, como referencia metodológica para los procesos de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información.

ISO/IEC 27701 (cuando aplique) – Extensión a ISO/IEC 27001 e ISO/IEC 27002 para gestión de información de privacidad, como referencia para la gestión de riesgos asociados al tratamiento de datos personales.

Políticas, manuales, procedimientos y lineamientos internos de la E.S.E. RAFAEL TOVAR POVEDA, incluyendo el Plan de Seguridad y Privacidad de la Información, el

Sistema de Gestión de la Calidad, el Modelo de Gestión del Riesgo institucional, el Reglamento Interno de Trabajo, el Manual de Funciones y los lineamientos de gestión documental y protección de datos personales adoptados por la entidad.

4. DEFINICIONES

A continuación, se presentan las definiciones de los términos más relevantes para la comprensión y aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Los términos se organizan en orden alfabético:

Activo de información: Cualquier información o elemento relacionado con su tratamiento (datos, sistemas, aplicaciones, soportes, edificios, equipos, procesos, personas, servicios, etc.) que tenga valor para la E.S.E. y deba ser protegido.

Afectación a la confidencialidad: Situación en la que la información es accedida, conocida o divulgada por personas, procesos o sistemas no autorizados.

Afectación a la disponibilidad: Situación en la que la información o los servicios asociados no están accesibles o utilizables por los usuarios autorizados cuando los requieren.

Afectación a la integridad: Situación en la que la información o los sistemas son modificados, alterados, eliminados o dañados de forma no autorizada, afectando su exactitud, completitud o vigencia.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daño a un activo de información o a la organización. Puede ser de origen interno o externo, intencional o accidental.

Análisis de riesgos: Proceso mediante el cual se comprende la naturaleza del riesgo y se determina el nivel de riesgo, a partir de la identificación de amenazas, vulnerabilidades, probabilidad e impacto sobre los activos de información.

Apetito de riesgo: Nivel y tipo de riesgo que la E.S.E. está dispuesta a asumir en función de sus objetivos institucionales, obligaciones legales y capacidades de tratamiento.

Control: Política, procedimiento, práctica, mecanismo técnico o estructura organizativa diseñada para modificar el riesgo, reduciendo la probabilidad de ocurrencia, el impacto o ambos.

Declaración de aplicabilidad: Documento que enumera los controles seleccionados para el tratamiento de riesgos de seguridad de la información, justificando su inclusión o exclusión, de acuerdo con los resultados de la evaluación y tratamiento de riesgos y con los controles de referencia (por ejemplo, el Anexo A de ISO/IEC 27001).

Impacto: Consecuencia o efecto que tendría la materialización de un riesgo sobre los objetivos institucionales, la prestación de servicios, la información o la imagen de la E.S.E. Puede expresarse en términos cualitativos o cuantitativos.

Incidente de seguridad de la información: Evento o conjunto de eventos no deseados o inesperados relacionados con la seguridad de la información que tienen una probabilidad significativa de comprometer la confidencialidad, integridad o disponibilidad de los activos de información.

Nivel de riesgo: Resultado de la combinación de la probabilidad de ocurrencia de un evento de riesgo y el impacto asociado a su materialización. Se utiliza para priorizar los riesgos y decidir las acciones de tratamiento.

Parte interesada: Persona, grupo u organización que puede afectar, verse afectada o percibirse como afectada por las decisiones o actividades relacionadas con la seguridad y privacidad de la información (por ejemplo: usuarios de servicios de salud, funcionarios, entes de control, proveedores, comunidad).

Plan de tratamiento de riesgos: Documento que define las acciones específicas para gestionar los riesgos de seguridad y privacidad de la información que se consideran inaceptables, indicando las opciones de tratamiento, controles seleccionados, responsables, plazos y recursos asociados.

Probabilidad: Estimación de la posibilidad de que una amenaza explote una vulnerabilidad y se materialice un riesgo, teniendo en cuenta la frecuencia observada, las condiciones actuales y los controles existentes.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo sobre un activo de información o sobre la organización. Es función de la probabilidad de ocurrencia y el impacto asociado.

Riesgo residual: Riesgo que permanece después de aplicar las medidas de tratamiento seleccionadas (controles), y que la organización decide aceptar, transferir, compartir o seguir tratando.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente, puede incluir otras propiedades como autenticidad, trazabilidad y confiabilidad.

SGSI (Sistema de Gestión de Seguridad de la Información): Conjunto de políticas, procedimientos, procesos, recursos y actividades interrelacionadas que permiten establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en la organización, con base en un enfoque de gestión del riesgo (por ejemplo, conforme a ISO/IEC 27001).

Tratamiento del riesgo: Proceso consistente en seleccionar e implementar una o más opciones para modificar el riesgo, tales como mitigarlo (reducirlo), evitarlo, transferirlo/compartirlo o, en algunos casos, aceptarlo formalmente.

Vulnerabilidad: Debilidad de un activo, de un control o de un proceso que puede ser explotada por una amenaza y, en consecuencia, aumentar la probabilidad o el impacto de un riesgo.

5. RESPONSABLES

Se describen a continuación los cargos y dependencias responsables de la planificación, ejecución, seguimiento y mejora del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la E.S.E. RAFAEL TOVAR POVEDA.

5.1 Gerencia

- Aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y sus actualizaciones.
- Definir el nivel de riesgo aceptable (apetito de riesgo) para la E.S.E. y validar las decisiones sobre riesgos residuales.

- Asignar los recursos humanos, tecnológicos, físicos y financieros necesarios para la implementación de las medidas de tratamiento de riesgos priorizadas.
- Presidir o delegar la participación en los espacios de revisión de resultados del análisis y tratamiento de riesgos y aprobar los planes de acción correspondientes.

5.2 Subgerencia Administrativa y Financiera

- Coordinar, junto con la Gerencia, la incorporación de las acciones de tratamiento de riesgos en los planes operativos y presupuestales de la E.S.E.
- Asegurar que las dependencias bajo su responsabilidad integren en su gestión las medidas de tratamiento de riesgos definidas en el Plan.
- Hacer seguimiento al cumplimiento de los plazos y responsables definidos en el Plan de Tratamiento de Riesgos para las áreas administrativas y de apoyo.

5.3 Oficina de Control Interno

- Liderar metodológicamente el proceso de identificación, análisis, evaluación y tratamiento de riesgos de seguridad y privacidad de la información.
- Proponer y mantener actualizada la metodología de gestión de riesgos, escalas de probabilidad e impacto, criterios de aceptación de riesgos y formatos de registro.
- Coordinar la elaboración, actualización y consolidación de la matriz de riesgos de seguridad y privacidad de la información y del Plan de Tratamiento de Riesgos.
- Verificar, mediante actividades de auditoría interna y seguimiento, el avance y eficacia de las acciones de tratamiento implementadas.
- Informar a la Gerencia y a los órganos de dirección sobre los riesgos críticos, riesgos no tratados y riesgos residuales que superen los niveles aceptables.

5.4 Oficina de Sistemas de Información

- Identificar, junto con Control Interno, las amenazas y vulnerabilidades de naturaleza tecnológica que afecten la confidencialidad, integridad y disponibilidad de la información.
- Proponer controles técnicos y operativos (configuración de equipos, redes, aplicaciones, respaldos, seguridad perimetral, monitoreo, etc.) como medidas de tratamiento de riesgos.
- Ejecutar las acciones de tratamiento de riesgos que correspondan a la infraestructura tecnológica, de acuerdo con lo definido en el Plan de Tratamiento de Riesgos.
- Mantener actualizada la información sobre activos tecnológicos, sistemas y servicios que constituya insumo para la identificación y valoración de riesgos.

5.5 **Responsables de procesos y propietarios de activos de información**

- Identificar los riesgos de seguridad y privacidad de la información asociados a los procesos y activos bajo su responsabilidad.
- Participar en las sesiones de análisis y valoración de riesgos, aportando información sobre causas, consecuencias y controles existentes.
- Definir, junto con Control Interno y Sistemas, las acciones de tratamiento de riesgos aplicables a sus procesos (controles organizacionales, procedimientos, ajustes operativos, etc.).
- Implementar y mantener las medidas de tratamiento de riesgos asignadas a su proceso, garantizando su incorporación en la operación diaria.
- Reportar a Control Interno y a la Gerencia las dificultades para implementar medidas de tratamiento, especialmente cuando se relacionen con limitaciones de recursos o cambios en el contexto.

5.6 Equipo de apoyo en gestión de la información (Calidad, Gestión Documental, u otros que se designen)

- Apoyar la identificación y clasificación de activos de información, así como la documentación de riesgos y controles asociados a la gestión documental y a la calidad de la información.
- Suministrar información estadística, indicadores y análisis que permitan valorar el impacto de los riesgos y la eficacia de las medidas de tratamiento.
- Colaborar en la elaboración y actualización de manuales, procedimientos y formatos que se deriven del Plan de Tratamiento de Riesgos.

5.7 Todos los usuarios de la E.S.E.

- Conocer y cumplir las políticas, procedimientos y controles definidos como parte del tratamiento de riesgos de seguridad y privacidad de la información.
- Reportar de manera oportuna a sus superiores, a la Oficina de Sistemas o a la Oficina de Control Interno cualquier situación que pueda constituir un riesgo o incidente de seguridad de la información.
- Colaborar en la implementación de las medidas de tratamiento de riesgos que les sean aplicables en el ejercicio de sus funciones.

6. DESARROLLO DEL DOCUMENTO

Se describe la secuencia de las actividades necesarias para identificar, analizar, valorar y tratar los riesgos de seguridad y privacidad de la información en la E.S.E. RAFAEL

TOVAR POVEDA, indicando cómo se deben realizar, quiénes son los responsables y cuáles son los registros resultantes de cada una de ellas.

El desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se basa en un enfoque de gestión de riesgos alineado con las buenas prácticas internacionales en seguridad de la información (familia ISO/IEC 27000) y con las directrices del Modelo Integrado de Planeación y Gestión – MIPG y de MinTIC para el tratamiento de riesgos de seguridad y privacidad de la información.

6.1 Preparación y planificación del proceso de tratamiento de riesgos

Actividad: Definir la planificación general del proceso de tratamiento de riesgos de seguridad y privacidad de la información, incluyendo alcance del ejercicio, calendario de trabajo, participantes, metodología y herramientas a utilizar.

Cómo se realiza:

1. La Oficina de Control Interno revisa y/o actualiza la metodología institucional de gestión de riesgos de seguridad y privacidad de la información (criterios de probabilidad, impacto, niveles de riesgo y criterios de aceptación).
2. Se define el alcance del ciclo de gestión de riesgos (procesos, sedes, sistemas de información, períodos de tiempo) y se identifica a los responsables de proceso y propietarios de activos que participarán.
3. Se acuerda un cronograma de trabajo para las fases de identificación, análisis, valoración y definición de tratamientos, articulado con el calendario institucional y el Plan de Seguridad y Privacidad de la Información.
4. Se seleccionan o actualizan las plantillas y herramientas que se emplearán (matriz de riesgos, formatos de talleres, registros de decisiones, etc.).
5. La planificación se socializa con los responsables de proceso y las áreas clave (Sistemas, Calidad, Gestión Documental, etc.).

Responsables:

- Oficina de Control Interno: líder metodológico, define la planificación y coordina el proceso.
- Gerencia y Subgerencia Administrativa y Financiera: aprueban el cronograma general y aseguran la participación de las áreas.
- Oficina de Sistemas de Información: apoya la definición del alcance en lo referente a activos tecnológicos y sistemas.

Registros resultantes:

- Documento o acta de planificación del proceso de tratamiento de riesgos.
- Versión vigente de la metodología institucional de gestión de riesgos de seguridad y privacidad de la información.
- Cronograma de trabajo con responsables y fechas tentativas.

6.2 Identificación de riesgos de seguridad y privacidad de la información

Actividad: Identificar de manera sistemática los riesgos de seguridad y privacidad de la información que puedan afectar los objetivos de los procesos y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

Cómo se realiza:

1. Se identifican y documentan los activos de información relevantes (información, aplicaciones, infraestructura, personas, servicios, procesos) con apoyo de los responsables de proceso y de la Oficina de Sistemas.
2. Para cada activo y proceso se analizan:

- Amenazas potenciales (errores humanos, fallas técnicas, accesos no autorizados, desastres, malware, fugas de información, etc.).
- Vulnerabilidades asociadas (controles inexistentes o débiles, falta de capacitación, ausencia de procedimientos, deficiencias técnicas, etc.).

3. Se describen los riesgos utilizando una redacción clara, habitual en gestión de riesgos (por ejemplo: “Pérdida de información clínica por fallas en copias de respaldo”, “Divulgación no autorizada de datos personales por manejo inadecuado de historias clínicas en soporte físico”).
4. Cuando sea necesario, se realizan talleres de identificación de riesgos con los equipos de trabajo de cada proceso.
5. Se clasifica cada riesgo según categoría (estratégico, operativo, tecnológico, financiero, etc.) de acuerdo con la metodología institucional.

Responsables:

- Oficina de Control Interno: coordina la identificación y consolida la información.
- Oficina de Sistemas de Información: identifica amenazas y vulnerabilidades tecnológicas.
- Responsables de procesos y propietarios de activos de información: aportan riesgos específicos de sus áreas.
- Equipo de apoyo (Calidad, Gestión Documental, Estadística): apoya la identificación en temas de información, calidad y datos.

Registros resultantes:

- Listado de activos de información relevantes para el análisis de riesgos.
- Matriz de identificación de riesgos de seguridad y privacidad de la información (riesgo, activo, amenaza, vulnerabilidad, categoría, proceso).
- Actas o memorias de talleres de identificación de riesgos (cuando aplique).

6.3 Análisis y valoración de probabilidad e impacto

Actividad: Analizar y valorar cada riesgo identificado en términos de probabilidad de ocurrencia e impacto potencial, con el fin de obtener un nivel de riesgo que permita priorizar el tratamiento.

Cómo se realiza:

1. Se aplican las definiciones y escalas institucionales de probabilidad e impacto (por ejemplo, de 1 a 5), considerando:

- Frecuencia histórica de eventos similares.
- Condiciones actuales de control.
- Entorno tecnológico, normativo y operativo.

2. Para el impacto, se tienen en cuenta efectos sobre:

- Prestación de servicios de salud.
- Cumplimiento legal y regulatorio (protección de datos, transparencia, archivo, etc.).
- Imagen institucional y confianza de usuarios y partes interesadas.
- Pérdidas económicas y afectación de la continuidad del servicio.

3. Se calcula el nivel de riesgo (por ejemplo, probabilidad x impacto) y se ubica cada riesgo en la matriz de colores o niveles (bajo, aceptable, alto, inaceptable) definida por la institución.
4. Cuando haya desacuerdo sobre la valoración, se discute en sesión con los responsables de proceso para llegar a un consenso informado.

Para la valoración cuantitativa de los riesgos, la E.S.E. RAFAEL TOVAR POVEDA adopta escalas de probabilidad e impacto en una escala de 1 a 5, así como una matriz de combinación probabilidad–impacto que permite determinar el nivel de riesgo (bajo, aceptable, alto, inaceptable) y las medidas de respuesta asociadas.

Las definiciones detalladas de probabilidad, impacto, la matriz de niveles de riesgo y las correspondientes medidas de respuesta se encuentran en el Anexo 1. Escalas de

probabilidad, impacto y matriz de nivel de riesgo para la valoración de riesgos de seguridad y privacidad de la información.

Responsables:

- Oficina de Control Interno: dirige el análisis, aplica las escalas definidas y consolida las valoraciones.
- Responsables de procesos y propietarios de activos: aportan información sobre frecuencia e impacto en sus procesos.
- Oficina de Sistemas de Información: analiza probabilidad e impacto de los riesgos tecnológicos.

Registros resultantes:

- Matriz de riesgos con campos de probabilidad, impacto y nivel de riesgo calculado.
- Evidencias de las sesiones de análisis (actas, memorias, registros de acuerdos).

6.4 Determinación del nivel de aceptación del riesgo y priorización

Actividad: Definir qué riesgos requieren tratamiento, cuáles pueden aceptarse y en qué orden de prioridad se abordarán.

Cómo se realiza:

Se comparan los niveles de riesgo obtenidos con los criterios de aceptación de riesgos establecidos por la E.S.E. (por ejemplo, riesgos “altos” e “inaceptables” no son aceptables; riesgos “bajos” pueden asumirse).

1. Se elabora un listado de riesgos priorizados, identificando:
- Riesgos que deben ser tratados de manera inmediata.
- Riesgos que requieren tratamiento programado.
- Riesgos que pueden ser aceptados con monitoreo.
2. Para los riesgos aceptados, se deja explícita la justificación y el nivel de riesgo residual que la Gerencia decide asumir.
3. Los riesgos que superen los niveles de aceptación establecidos se resaltan como insumo obligatorio para la elaboración del Plan de Tratamiento de Riesgos.

La clasificación del nivel de riesgo (bajo, aceptable, alto, inaceptable) y las medidas generales de respuesta asociadas se encuentran definidas en el Anexo 1. Escalas de probabilidad, impacto y matriz de nivel de riesgo para la valoración de riesgos de seguridad y privacidad de la información

Responsables:

- Oficina de Control Interno: propone la priorización de riesgos y consolida el listado de tratamiento.
- Gerencia y Subgerencia Administrativa y Financiera: validan los criterios de aceptación y aprueban los riesgos que se aceptan y los que se tratarán.
- Responsables de procesos: participan en la priorización y en la justificación de la aceptación de riesgos en sus áreas.

Registros resultantes:

- Listado de riesgos priorizados para tratamiento, con indicación del nivel de riesgo.
- Registro de riesgos aceptados, con su justificación y decisión aprobada por la Gerencia.

6.5 Definición de opciones y acciones de tratamiento de riesgos

Actividad: Definir para cada riesgo priorizado las opciones de tratamiento (evitar, mitigar, transferir/compartir, aceptar) y las acciones concretas que se implementarán.

Cómo se realiza:

1. Para cada riesgo priorizado, se define la opción de tratamiento más adecuada:

- Evitar: modificar procesos o actividades para eliminar la fuente del riesgo.
- Mitigar: implementar controles que reduzcan probabilidad y/o impacto.
- Transferir/compartir: contratar seguros, acuerdos con terceros, etc.
- Aceptar: asumir conscientemente el riesgo residual.

2. Se describen las medidas de tratamiento concretas:

- Controles organizacionales (políticas, procedimientos, segregación de funciones).
- Controles tecnológicos (configuraciones seguras, autenticación, cifrado, respaldos, etc.).
- Controles físicos (accesos, cerraduras, cámaras, infraestructura).
- Acciones de formación y concientización.

3. Se asignan responsables, plazos tentativos y recursos requeridos para cada medida.
4. Cuando se requiera un nivel de especialización alto (por ejemplo, pruebas de penetración, diseño de arquitecturas de seguridad complejas), se evalúa la necesidad de apoyo externo especializado.

Responsables:

- Oficina de Control Interno: coordina la definición de opciones de tratamiento y verifica su coherencia con los niveles de riesgo.
- Oficina de Sistemas de Información: propone y detalla controles tecnológicos.
- Responsables de procesos: definen y asumen controles organizacionales y operativos.
- Gerencia y Subgerencia Administrativa y Financiera: validan las medidas que implican recursos significativos o cambios relevantes en procesos.

Registros resultantes:

- Matriz preliminar de Plan de Tratamiento de Riesgos (riesgo, opción de tratamiento, medidas, responsables, plazos, recursos).
- Actas o memorias de sesiones de trabajo donde se definieron los tratamientos.

6.6 Elaboración, aprobación y actualización del Plan de Tratamiento de Riesgos

Actividad: Consolidar, formalizar y mantener actualizado el documento “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información” y sus matrices asociadas.

Cómo se realiza:

1. Con base en la matriz preliminar, se elabora el Plan de Tratamiento de Riesgos en el formato institucional, incorporando:

- Riesgos priorizados.
- Medidas de tratamiento.
- Responsables, plazos, recursos y productos esperados.

2. Se revisa el borrador con los responsables de procesos, la Oficina de Sistemas y el equipo de apoyo para verificar su viabilidad técnica y operativa.
3. La Oficina de Control Interno ajusta el documento según observaciones y lo presenta a la Gerencia y a la Subgerencia Administrativa para su aprobación.
4. Una vez aprobado, el Plan se comunica a los responsables de su ejecución y se integra con el cronograma de actividades del Plan de Seguridad y Privacidad de la Información.
5. El Plan se revisa y actualiza al menos una vez al año o cuando ocurran cambios significativos en los riesgos, procesos, sistemas o normatividad.

Responsables:

- Oficina de Control Interno: consolida, redacta, actualiza y custodia el Plan de Tratamiento de Riesgos.
- Gerencia y Subgerencia Administrativa y Financiera: revisan y aprueban el documento y sus actualizaciones.
- Responsables de procesos y Oficina de Sistemas: revisan y validan la viabilidad de las acciones propuestas.

Registros resultantes:

- Documento formal del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aprobado.
- Versiones históricas del Plan, con su respectivo control de cambios.

6.7 Implementación y seguimiento de las medidas de tratamiento

Actividad: Ejecutar las acciones definidas en el Plan de Tratamiento de Riesgos y hacer seguimiento a su avance y eficacia.

Cómo se realiza:

1. Cada responsable de proceso y de área ejecuta las medidas asignadas en los plazos definidos (elaboración de procedimientos, implementación de controles, capacitación, adecuaciones, configuraciones, etc.).
2. La Oficina de Control Interno y la Subgerencia Administrativa solicitan reportes periódicos de avance sobre las acciones de tratamiento.
3. Se registran las evidencias de ejecución de cada medida (actas, procedimientos, capturas de pantalla, informes técnicos, certificados de capacitación, etc.).
4. Se actualiza periódicamente el estado de cada acción en la matriz del Plan (pendiente, en ejecución, ejecutada, no ejecutada, reprogramada).
5. Cuando una acción no pueda ejecutarse por falta de recursos u otras limitaciones, se documenta la situación y se evalúa el riesgo residual resultante para su elevación a la Gerencia.

Responsables:

- Responsables de procesos y propietarios de activos de información: ejecutan las medidas que les corresponden y reportan avances.
- Oficina de Sistemas de Información: implementa acciones técnicas (controles, configuraciones, herramientas, etc.).

- Oficina de Control Interno: consolida avances, verifica evidencias y reporta a la Gerencia.
- Gerencia y Subgerencia Administrativa y Financiera: toman decisiones frente a medidas no ejecutadas o que requieren recursos adicionales.

Registros resultantes:

- Matriz de seguimiento del Plan de Tratamiento de Riesgos (estado de acciones).
- Evidencias de ejecución de acciones de tratamiento (documentos, informes, registros, evidencias técnicas).

6.8 Revisión de resultados, riesgo residual y mejora continua

Actividad: Revisar periódicamente los resultados del tratamiento de riesgos, valorar el riesgo residual y definir acciones de mejora continua.

Cómo se realiza:

1. Una vez implementadas las medidas de tratamiento más relevantes, se realiza una revaloración de los riesgos para determinar el riesgo residual (probabilidad e impacto después del tratamiento).
2. Se compara el riesgo residual con los criterios de aceptación para verificar si se encuentra dentro de niveles tolerables.
3. Se identifican medidas adicionales cuando el riesgo residual permanece por encima de los niveles aceptables.
4. Los resultados del tratamiento y de la revaloración se presentan a la Gerencia y, cuando aplique, al Comité de Seguridad de la Información para la toma de decisiones.
5. Se actualizan el Plan de Tratamiento de Riesgos, la matriz de riesgos y, cuando corresponda, otros documentos del Sistema de Gestión de Seguridad de la Información.

Responsables:

- Oficina de Control Interno: coordina la revaloración de riesgos, consolida la información y propone ajustes al Plan.
- Responsables de procesos y Oficina de Sistemas de Información: aportan información sobre efectividad de controles y cambios en el entorno.
- Gerencia: decide sobre aceptación de riesgos residuales altos y sobre nuevas medidas de tratamiento.

Registros resultantes:

- Matriz de riesgos actualizada con riesgo residual.
- Informes de revisión de resultados del tratamiento de riesgos.
- Actas de decisiones de la Gerencia y/o Comité de Seguridad de la Información.
- Actualizaciones del Plan de Tratamiento de Riesgos y del control de cambios.

7. CRONOGRAMA DE ACTIVIDADES

El cronograma de actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es la herramienta de planificación que organiza, en el tiempo, las acciones necesarias para identificar, valorar y tratar los riesgos que afectan la confidencialidad, integridad, disponibilidad y privacidad de la información de la E.S.E.

Su propósito es:

- Visualizar las actividades que deben ejecutarse para implementar las medidas de tratamiento de riesgos.
- Definir responsables, plazos y recursos requeridos.
- Facilitar el seguimiento al avance de las acciones y el cierre de los riesgos intervenidos.
- Asegurar la articulación entre el Plan de Tratamiento de Riesgos, el SGSI y los demás sistemas de gestión institucional.

Las actividades del plan deben quedar soportadas en el **cronograma de actividades** y registradas como anexo en el formato institucional: **"Planeación Anual de Actividades – Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información"**.

7.1 Lineamientos para la elaboración del cronograma

Para la construcción y actualización del cronograma de actividades se tendrán en cuenta, como mínimo, los siguientes criterios:

1. **Fuente de las actividades**
   Las actividades a programar se derivan de:
   - Los resultados de la identificación, análisis y valoración de riesgos.
   - El Plan de Tratamiento de Riesgos y la Declaración de Aplicabilidad.
   - Las recomendaciones de auditorías internas y externas.
   - Las decisiones del Comité de Seguridad de la Información y de la Gerencia.
2. **Planeación anual y actualización**

- El cronograma se elaborará, como mínimo, para un periodo **anual**, pudiendo ajustarse cuando se presenten cambios significativos en los riesgos, controles, procesos o infraestructura tecnológica.
- Las actividades deben distribuirse en el año de manera realista, considerando la capacidad operativa de las dependencias responsables.

3. **Contenido mínimo de cada actividad**
   Cada fila o ítem del cronograma debe incluir, al menos:
   - Descripción de la actividad de tratamiento o seguimiento del riesgo.
   - Dependencia responsable y responsable directo.
   - Riesgo(s) asociado(s) y relación con el Plan (numeral correspondiente).
   - Periodo de ejecución (fecha de inicio y fecha de fin) y frecuencia.
   - Recursos requeridos (humanos, tecnológicos, físicos y/o financieros).
   - Producto o evidencia esperada (matriz actualizada, informe, acta, registro, etc.).
   - Indicador o criterio de cumplimiento (por ejemplo: % de riesgos tratados, % de acciones ejecutadas, etc.).
4. **Aprobación y seguimiento**
   - El cronograma será consolidado por la Oficina de Control Interno, con apoyo de la Oficina de Sistemas y los líderes de proceso.
   - Será revisado por el Comité de Seguridad de la Información (cuando exista) y aprobado por la Gerencia.
   - El avance de las actividades será revisado periódicamente (trimestral o semestralmente) y se dejará constancia en actas o informes de seguimiento, incluyendo ajustes, reprogramaciones y justificación de actividades no ejecutadas.

7.2 Anexo: Formato Planeación Anual de Actividades

Las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información deberán registrarse en el formato institucional:
“Planeación Anual de Actividades – Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”, el cual hará parte integral del presente Plan como anexo y será el documento de referencia para:

- Programar anualmente las actividades de tratamiento y seguimiento de riesgos.
- Registrar responsables, periodos de ejecución, recursos y evidencias.
- Hacer seguimiento al cumplimiento de las acciones definidas y al cierre de los riesgos intervenidos.

La Gerencia y la Subgerencia Administrativa deberán asegurar que el cronograma cuente con la asignación de los recursos mínimos necesarios para su ejecución y, cuando no sea posible asignarlos en el tiempo requerido, esta situación se registrará como riesgo residual en la matriz de riesgos y/o en las actas del Comité de Seguridad de la Información.

8. INDICADORES

NOMBRE DEL INDICADOR	INTERPRETACIÓN	FORMULA	META
Porcentaje de riesgos de seguridad y privacidad de la información tratados	Mide el nivel de avance institucional en la implementación de las acciones definidas en el Plan de Tratamiento de Riesgos.	Número de riesgos con tratamiento implementado / Número total de riesgos priorizados para tratamiento x 100	100 %.
Porcentaje de acciones del Plan de Tratamiento de Riesgos ejecutadas en el plazo establecido		Número de acciones ejecutadas dentro del plazo / Numero total de actividades programadas x 100	≥ 90 %

9. BIBLIOGRAFIA

- Constitución Política de Colombia. (1991). Constitución Política de Colombia.
- Departamento Administrativo de la Función Pública. (s. f.). Modelo Integrado de Planeación y Gestión – MIPG. Lineamientos para la gestión de riesgos de seguridad y privacidad de la información. Bogotá, Colombia.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
- International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. ISO.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Diario Oficial de la República de Colombia.

- Ley 1437 de 2011. Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Diario Oficial de la República de Colombia.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial de la República de Colombia.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Diario Oficial de la República de Colombia.
- Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos. Diario Oficial de la República de Colombia.

- Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.). Guía de gestión y tratamiento de riesgos de seguridad y privacidad de la información. MinTIC, República de Colombia.
- Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.). Guía para la implementación de la seguridad y privacidad de la información en entidades públicas. MinTIC, República de Colombia.

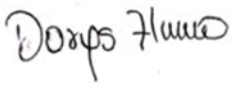
- Archivo General de la Nación. (2015). Acuerdo 03 de 2015. Lineamientos generales sobre la gestión de documentos electrónicos. Archivo General de la Nación, República de Colombia.

10. ANEXOS

Anexo 1. Formato matriz de riesgo. Código: ES-PGC-SOGC-F020
Anexo 2. Planeación Anual de Actividades – Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
Anexo 3. Manual de Gestión del Riesgo Institucional Código: ES-PGC-DE-M001

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión	**Descripción del Cambio**	**Fecha de aprobación**
01	Elaboración del documento	18/01/2021
02	Se ajusta documento por programa de auditoria para el mejoramiento continuo Pamec. Se ajusta objetivos, alcance, responsables, normatividad, se agrega en procedimiento describiendo la secuencia de las actividades necesarias para identificar, analizar, valorar y tratar los riesgos de seguridad y privacidad de la información. Por ultimo se ajusta plantilla según nueva versión del manual de gestión documental de calidad.	27/1/2026

Elaborado por:	Revisado por:	Aprobado por:
Firma: 	Firma: 	Firma: 
Nombre: Juan Camilo Guevara Plazas Cargo: Ingeniero de Sistemas	Nombre: Dorys Enith Almario Estrada Cargo: Asesora de Calidad	Nombre: Maydi Nayive Collazos Medina Cargo: Subgerencia Administrativa y Financiera.