FECHA DEL CAMBIO	DESCRIPCIÓN DEL CAMBIO	JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
23/06/2020	Creación del documento	NA	1
31/08/2023	Ajuste Documento	Ajuste acuerdo a Normatividad Vigente	2
28/11/2025	Actualización del documento por normatividad	Ajuste acorde a manuales MINTIC y gobierno digital	3

1. OBJETIVO

Establecer un marco de referencia sistemático y escalable, basado en estándares reconocidos como ISO 27001, para la identificación, análisis, evaluación y tratamiento continuo de los riesgos de Seguridad y Privacidad de la Información (SPI). El objetivo final es reducir la exposición a amenazas que comprometan la confidencialidad, integridad y disponibilidad de los datos de los pacientes y la información crítica de la institución, garantizando el cumplimiento normativo y respaldando la continuidad de la prestación de servicios de salud.

2. ALCANCE

Este Plan aplica a todos los procesos, sistemas de información, activos tecnológicos, y personal (incluyendo terceros y contratistas) que manejen, procesen o almacenen Información Confidencial y Sensible, especialmente la Historia Clínica Electrónica (HCE) y los datos personales de pacientes y colaboradores, dentro de la institución.

3. RESPONSABLES

- Gerente
- Líderes de Proceso
- Gestión de la Información y comunicación Organizacional
- Todos los colaboradores

4. SOPORTE LEGAL

- **Ley 57 de 1985:** Publicidad de los actos y documentos oficiales.
- **Ley 527 de 1999:** 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.
- **Ley 594 de 2000:** Ley General de Archivos.
- **Ley 1266 de 2008:** Disposiciones generales de habeas data y se regula el manejo de

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

la información.

- **Ley 1437 de 2011:** Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 1474 de 2011:** Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
- **Ley estatutaria 1581 de 2012:** Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- **Ley estatutaria 1618 de 2013:** Ejercicio pleno de las personas con discapacidad.
- **Ley 1712 de 2014:** Ley de Transparencia y acceso a la información pública. Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
- **Ley Estatutaria 1757 de 2015:** Promoción y protección del derecho a la participación democrática.
- **Ley 2015 de 2020:** Regulación de la Interoperabilidad de la Historia Clínica Electrónica (HCE). Es indispensable para la gestión de datos en salud.

Decretos, Acuerdos y Resoluciones

- **Resolución 1995 de 1999:** Establece normas para el manejo y conservación de la Historia Clínica (aplica a su formato digital, plazos de reserva y reglas de acceso).
- **Decreto 1747 de 2000:** Entidades de certificación, los certificados y las firmas digitales.
- **Decreto 019 de 2012:** Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Decreto Único Reglamentario 1078 de 2015:** Del Sector de Tecnologías de la Información y las Comunicaciones (consolida gran parte de la normativa de TIC, incluyendo el Modelo de Seguridad y Privacidad de la Información y su Título 9 sobre seguridad digital).
- **Decreto Único Reglamentario 1081 de 2015:** Del Sector Presidencia de la República (consolida la reglamentación sobre la gestión de la información pública).
- **Acuerdo 03 de 2015:** del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
- **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

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

Estado".

- **CONPES 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital (Marco de alto nivel para la estrategia de ciberseguridad).
- **Resolución 500 de 2021:** "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

Estándares Internacionales y Nacionales

- **NTC/ISO 31000:2009:** Gestión del Riesgo. Principios y directrices.
- **NTC/ ISO 27001:2013:** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

5. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Activo de Información:** Todo lo que tiene valor para la organización. Hay varios tipos de activos entre los que se incluyen: Información, Software, como un programa de cómputo, Físico, como un computador, Servicios, Personas, sus calificaciones, habilidades y experiencia, Intangibles, tales como la reputación y la imagen.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación.
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

el riesgo se materializa.

- **Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Confidencial:** Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Disponibilidad:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

desconocida previamente que puede ser pertinente a la seguridad.

- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Gestión de incidentes de Seguridad de la Información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos.
- **Incidente de seguridad de la información:** Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
- **Integridad:** Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado.
- **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.
- **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

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

las diferentes auditorías de los sistemas integrados de gestión.

- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de Seguridad de la Información inaceptables e implantar los controles necesarios para proteger la información
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- **Propietario del Riesgo:** Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo particular, incluyendo la implementación de acciones de tratamiento.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo de Privacidad:** Riesgo asociado a la vulneración de los derechos de los Titulares de los Datos (Acceso, Rectificación, Supresión, etc.) o al incumplimiento de la Ley 1581/2012, resultando en daños reputacionales o sanciones.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

objetivos o la misión institucional.

- **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.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Tratamiento del Riesgo:** controlar todos los riesgos que se identifican durante la evaluación del riesgo, en la mayoría de los casos esto significa una disminución de riesgos con lo que disminuye la probabilidad de tener un incidente, además se reduce el impacto que generan los activos.
- **Tolerancia al Riesgo:** La cantidad y tipo de riesgo que la organización está dispuesta a buscar, retener o aceptar en pos de lograr sus objetivos. Define el umbral de riesgo aceptable.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.
- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información.

6. DESARROLLO

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía N° 7 Gestión de riesgos y la Guía N° 8 Controles de seguridad de la información del Ministerio de Tecnologías de la Información y las comunicaciones – MINTIC.

En la siguiente imagen se muestra el procedimiento de la Guía N° 7 que propone el Departamento administrativo de la función pública (DAFP) en concordancia con el Ministerio de Tecnologías de la información y comunicaciones (MinTIC) para la gestión de riesgos de Seguridad de Información.

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

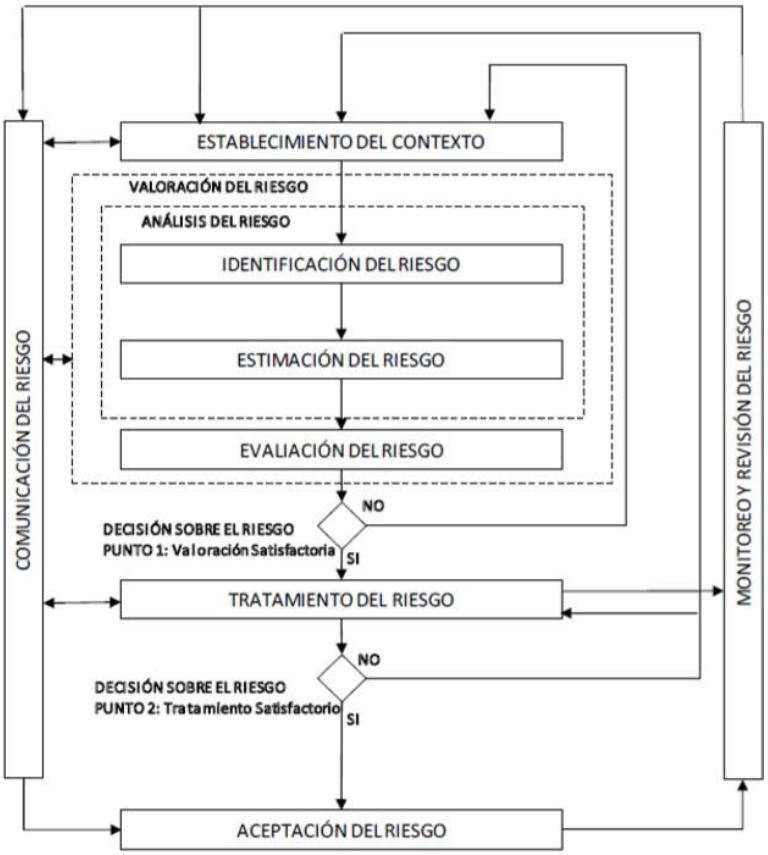

Imagen 2. Tomado de la NTC-ISO/IEC 27005

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Los activos de información se clasifican en dos tipos:

a. Primarios:

- **Procesos o subprocesos y actividades de la entidad:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización.
- **Información:** información que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados; información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

periodo de tiempo.

- **Actividades y procesos de negocio:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b. De Soporte

- **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos y los colaboradores en el desarrollo de sus tareas diarias.
- **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos y en marcan la información recolectada de los colaboradores, usuarios y sus familias.
- **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores y/o teléfonos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.).
- **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, colaboradores, responsables, etc.).

Criterio de Valoración de Activos Confidencialidad, Integridad, Disponibilidad.

Antes de proceder, es indispensable establecer la valoración de cada activo en términos de los atributos fundamentales de seguridad:

Atributo	Definición	Criterio de Riesgo
Confidencialidad	La información no debe ser revelada a procesos o personas no autorizadas.	Alto: Si se compromete, resultan sanciones legales (Ley 1581/2012) y pérdida de confianza del paciente.
Integridad	La información debe ser exacta y completa.	Alto e: Si se compromete, afecta la calidad de la atención médica y puede poner en riesgo la vida del paciente (ej. Error de diagnóstico por dato alterado).

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

Disponibilidad	El acceso a la información y sistemas debe ser oportuno cuando se requiera.	Alto: Si se compromete, interrumpe la prestación de servicios esenciales (ej. Urgencias no puede acceder a Historia Clínica).

ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presentan las etapas a desarrollar durante la administración del riesgo.

1. **Contexto para la gestión del riesgo:** Determinar los factores que afectan el riesgo. (incluye la definición de la Tolerancia al Riesgo).
2. **Identificación de Riesgos:** Identificar las causas, riesgo, consecuencias y clasificación del riesgo. (incluye el análisis de Amenazas y Vulnerabilidades).
3. **Análisis:** Calificación y evaluación del riesgo. (Riesgo Inherente).
4. **Valoración:** Identificación y evaluación de controles. (Cálculo del Riesgo Residual).
5. **Manejo:** Determinar, las acciones para el fortalecimiento de los controles. (Tratamiento).
6. **Seguimiento:** Evaluación integral de los riesgos.

Contexto para la gestión del riesgo

Definir el contexto para la gestión del riesgo marca la ruta que la ESE Salud del Tundama debe asumir frente a la exposición del riesgo, ya que permite conocer las situaciones que pueden afectar el cumplimiento de los objetivos de seguridad y privacidad de la información desde la estructura organizacional, los recursos físicos y tecnológicos.

- **Tolerancia al Riesgo:** Se debe definir explícitamente el umbral de riesgo aceptable.
- **Riesgo Aceptable:** Riesgos clasificados en zona **Baja (B)**. Estos riesgos se monitorean, pero no requieren acciones inmediatas de tratamiento.
- **Riesgo No Aceptable:** Riesgos clasificados en zonas **Moderada (M), Alta (A), y Extrema (E)**. Estos deben ser tratados para reducir su nivel hasta una zona de riesgo Baja.

Identificación de riesgos

El propósito de esta etapa permite conocer los potenciales eventos, estén o no bajo el

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

control de la ESE Salud del Tundama, los cuales ponen en riesgo el logro de su misión, estableciendo las causas y los efectos que lo generan. Adicionalmente, en esta etapa también se realiza la clasificación del riesgo.

	Causas	**Riesgos**	**Consecuencia**	**Clasificación**	**Resultado**
Componentes	Medios o circunstancias	Evento que tendrá un impacto	Efecto que se puede presentar	De acuerdo a las características	Identificación del Riesgo

Como resultado de esta fase se obtendrán:

- Un análisis detallado de los activos relevantes de seguridad.
- Un estudio de las posibles amenazas sobre los sistemas de información, así como su impacto.

DESCRIPCIÓN DE VULNERABILIDADES

Las vulnerabilidades son debilidades internas que la entidad puede controlar.

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la ESE Salud del Tundama se encuentra otras amenazas e impactos como los siguientes:

Vulnerabilidades y Amenazas identificadas en la ESE (mejoradas):

- **Puntos de red insuficientes:** Conexiones no controladas o improvisadas que pueden eludir la seguridad perimetral.
- **Riesgo de pérdida de información por desconexión accidental:** Cableado eléctrico inadecuado que expone a fallas de energía súbitas.
- **Incumplimiento del cuidado de activos:** (ej. Bebidas cerca de equipos, reutilización de papeles con información reservada). Vulnerabilidad de Confidencialidad y Disponibilidad.
- **Uso de dispositivos de almacenamiento personales (USB/discos portátiles):** Riesgo de fuga de información y/o ingreso de *malware*. Vulnerabilidad de Confidencialidad e Integridad.
- **Falta de control para el uso de portátiles:** Exponiendo la red a virus y la información

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

a pérdidas por *hardware* no controlado.

- **Ausencia de historial de asistencias y/o mitigación de vulnerabilidades:** Dificulta el seguimiento de la efectividad de los controles.
- **Documentos físicos sin digitalizar:** Expuestos a pérdidas y daños físicos debido a sitios de almacenamiento inadecuados. Vulnerabilidad de Integridad y Disponibilidad.

a) Causas del riesgo

Uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

- **Lluvia de ideas**: usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos.
- **Diagrama Causa-efecto (Espina de pescado):** es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo mediante el análisis desde los factores generadores de riesgo.

b) Consecuencias de los riesgos

Son los efectos que pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la ESE Salud del Tundama, generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio entre otras.

c) Clasificación de los riesgos

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

Clases de riesgo	Definición
Estratégico	Relacionados con la misión y el cumplimiento de los objetivos estratégicos de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad.
Financieros	Relacionados con el manejo de los recursos de la entidad.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras para el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

Adaptado de guía para administración de riesgo DAFP 2018

1. Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener el Nivel de Riesgo Inherente (antes de controles).

Escala para calificar la probabilidad del riesgo

Nivel	Concepto	Frecuencia
Raro (1)	Imposible que ocurra (Lleva más de 5 años sin ocurrir).	No ha ocurrido en los últimos cinco años.
Improbable (2)	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
Ocasional (3)	El evento podría ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
Probable (4)	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
Casi Seguro (5)	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Adaptado para la ESE Salud del Tundama de la Guía de Riesgos DAFP, 2018

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

Escala para calificar el impacto del riesgo

Nivel de Impacto	Estratégico	Operativo	Financieros	Cumplimiento	Imagen
INSIGNIFICANTE (1)	Efectos mínimos sobre la ESE.	Afecta el cumplimiento de algunas actividades.	Genera ajustes a una actividad concreta.	Genera un requerimiento.	Afecta a un grupo de servidores del proceso.
MENOR (2)	Bajo impacto o efecto sobre la ESE.	Afecta el cumplimiento de las metas del proceso.	Genera ajustes en los procedimientos.	Genera investigaciones disciplinarias.	Afecta a los servidores del proceso.
MODERADO (3)	Medianas consecuencias o efectos sobre la ESE.	Afecta las metas de un grupo de procesos.	La pérdida afecta considerablemente la prestación del servicio.	Genera interrupciones en la prestación del servicio.	Afecta a todos los servidores de la ESE.
MAYOR (4)	Altas consecuencias o efectos sobre la ESE.	Afecta el cumplimiento de las metas de la ESE.	La pérdida afecta considerablemente el presupuesto de la ESE.	Genera sanciones.	Afecta a toda la entidad.
CATASTRÓFICO (5)	Desastrosas consecuencias o efectos sobre la ESE.	Genera paro total de la ESE.	Afecta al presupuesto de otras entidades o del departamento.	Genera cierre definitivo de la ESE.	Afecta al Departamento, Gobierno, todos los usuarios de la ESE.

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

a- Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

PROBABILIDAD	IMPACTO				
	Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Ocasional	B	M	A	A	E
Probable	M	A	A	E	E
Casi Seguro	M	A	E	E	E

Color	Zona de riesgo
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Adaptado de guía para administración de riesgo DAFP 2011

Valoración de los Riesgos (Riesgo Residual)

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos, en tres momentos:

1. Identificando los Controles: Acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo.

2. Evaluación de Controles: Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo.

3. Riesgo Residual y Definición de Opciones de Manejo: Se recalcula el riesgo (P x I) posterior a la aplicación de los controles para obtener el Riesgo Residual.

1. Manejo de riesgos (Tratamiento)

Una vez determinada la zona donde está ubicado el Riesgo Residual, y dependiendo de las opciones de manejo (Mitigar/Reducir, Transferir/Compartir, Evitar, Aceptar), se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados.

Acción a Desarrollar	+	Definición de responsables	+	Definición de Plazo	=	Definición Adecuada de Acciones
Resolución adecuada de los Riesgos						Resultado esperado

Si el Riesgo Residual se ubica en la zona baja (B), el manejo estará enfocado en garantizar que los controles operan de manera adecuada. Los riesgos ubicados en las

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

zonas moderada, alta o extrema, exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

2. Seguimiento de riesgos (Monitoreo)

Cuando sea solicitado por el comité, Se presentarán avances sobre el funcionamiento y manejo de los riesgos en la administración en cuanto al cumplimiento de las políticas y directrices para la administración del riesgo. Los resultados de la evaluación y las observaciones deben ser posteriormente solucionados y entregados a la gerencia, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo

PROPUESTA DE SEGURIDAD (Acciones de Mitigación)

Seguridad Física y Eléctrica:

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Implementar y hacer seguimiento a la política de "Escritorio Limpio y Pantalla Despejada" para mitigar derrames de líquidos y exposición de información física/digital.

Seguridad Lógica y de Datos:

- Establecer y socializar políticas de seguridad y privacidad de la información (incluyendo el uso de Historia Clínica y la prohibición de uso de dispositivos personales como USB).
- Implementar controles de acceso estricto (Principio de Mínimo Privilegio) para restringir el acceso del personal solo a los sistemas y datos estrictamente necesarios para su función.

PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD (Disponibilidad)

- Obtener un servicio de nube dedicado o un sistema de backup inmutable (off-site) para la información de la ESE Salud del Tundama con el fin de tener un respaldo

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

en caso de accidentes catastróficos.

- Realizar pruebas periódicas de restauración de copias de seguridad (pruebas de Disaster Recovery) para asegurar que la información es íntegra y disponible.

PLAN DE CONTINUIDAD (Disponibilidad y Recuperación)

- Socializar con los colaboradores de la ESE Salud del Tundama la importancia del Plan de Contingencia y los procedimientos a seguir ante un incidente grave de seguridad.

- Diseñar estrategias para el proceso de recuperación, definiendo claramente los Objetivos de Tiempo de Recuperación y Objetivos de Punto de Recuperación.

- **Estrategia de Mitigación:** La posición prioritaria es la Mitigación del Riesgo mediante el diseño de controles y la implementación de acciones correctivas y preventivas.

PLAN DE CAPACITACIÓN

Contar con un plan de capacitación continua para el personal:

- Elaborar un programa de capacitación en temas de Ciberseguridad, Privacidad (Ley 1581), y Políticas de Seguridad de la Información para todos los colaboradores de la ESE Salud del Tundama, con énfasis en el manejo de Historia Clínica.
- Fortalecer la capacidad del personal de sistemas para realizar análisis de vulnerabilidades.

CRONOGRAMA DE IMPLEMENTACION DE RIESGOS

Este cronograma establece un plan de trabajo de 12 meses, estructurado en cuatro fases clave para garantizar una implementación progresiva y efectiva de los controles.

FASE	ACTIVIDADES	RESULTADO ESPERADO	PLAZO	RESPONSABLE
Base				
1	Revisar y actualizar de ser necesario los documentos relacionados con	Documentos actualizados	2 meses	Gerencia de la Información

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

	seguridad y privacidad.			
2	Definir el nivel de riesgo que estamos dispuestos a aceptar.	Documento con el "Umbral Aceptable de Riesgo".	1 mes	Gerencia de la Información
3	Terminar de identificar y calificar todos los problemas de riesgo (Riesgo Inicial).	La Matriz de Riesgos con los problemas calificados.	1 mes	Gerencia de la Información / Líder Gestión del Riesgo
Soluciones Urgentes				
1	Asegurar contraseñas seguras en los softwares	Más del 70% de usuarios.	2 meses	Gerencia de la Información
2	Revisar y garantizar el Respaldo de Datos Seguro y Externo (Backup Inmutable).	Prueba exitosa de recuperación de datos críticos.	1 mes	Gerencia de la Información
3	Revisar y Limitar los Permisos de Acceso. Cada persona solo accede a lo que necesita.	Lista de accesos verificada por cada jefe de área.	1 mes	Gerencia de la Información / Lideres de Proceso
Crecimiento y Preparación				
1	Crear y Socializar el Plan de contingencia y Plan de seguridad de la información para seguir trabajando si hay un desastre (Plan de Continuidad).	Plan de Continuidad de Negocio aprobado y conocido por todos.	1 mes	Gerencia de la Información / todos los Colaboradores
2	Jornada de Capacitación sobre virus, contraseñas seguras y el manejo de la Historia Clínica.	Registro de asistencia y nota > 80% en la evaluación de conocimiento.	1 mes	Gerencia de la Información / todos los Colaboradores
3	Arreglo y organización de cuartos de sistemas y puntos de red.	Informe de cumplimiento de Seguridad Física.	6 meses	Gerencia de la Información / todos los Colaboradores
Revisión y Cierre				
1	Auditoría Interna para revisar si las nuevas medidas están funcionando.	Informe de No Conformidades.	2 mes	Auditoría Interna
2	Corregir los problemas encontrados en la auditoría y ajustar el Plan de Riesgos.	Matriz de Riesgos con el Riesgo Restante (Residual) en nivel Bajo.	1 mes	Gerencia de la Información / Líder Gestión del Riesgo

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.

Elaborado por: Edwin Andrés Romero Agudelo	**Cargo:** Líder Sistemas de la Información	**Fecha:** 23/06/2020
Ultima Actualización: Edwin Andrés Romero Agudelo	**Cargo:** Líder de Información y Comunicación Organizacional	**Fecha:** 02/12/2025 **Firma:**
Revisado por: Sandra Victoria Avendaño Merchán	**Cargo:** Líder de Mejoramiento Continuo	**Fecha:** 02/12/2025 **Firma:**
Aprobado por: Andrea Liliana Arias Perdomo	**Cargo:** Gerente	**Fecha:** 02/12/2025 **Firma:**

Este documento es propiedad de la Empresa Social del Estado Salud del Tundama. Prohibida su Reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Salud del Tundama.