FECHA DEL CAMBIO	DESCRIPCIÓN DEL CAMBIO	JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
23/06/2020	Elaboración del documento	N.A.	1
31/08/2023	Ajuste documento	Ajuste de acuerdo a las normativas vigentes	2

1. OBJETIVO

Establecer los conceptos básicos y metodológicos para mantener la integridad, confidencialidad y disponibilidad de la información a través de una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la ESE Salud del Tundama.

2. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

3. RESPONSABLES

- Gerente
- Líderes de Proceso
- Gestión de la Información y comunicación Organizacional

4. SOPORTE LEGAL

- Decreto 338 de 2022: "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

- Resolución 746 del 11 de marzo de 2022, "por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

- Decreto 767 de 2022, mediante el cual se actualizó la política de Gobierno Digital del país.

- 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".

- Resolución 1519 del 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

- Ley 1915 Julio 12 de 2018 Disposiciones relativas al derecho de autor y los derechos conexos.

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.

- Acuerdo 03 de 2015 “Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012”

- Ley 1712 marzo 06 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Decreto 886 mayo 13 de 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

- Decreto 2364 de 2012 - Firma electrónica.

- Ley Estatutaria 1581 de 2012 - Protección de datos personales.

- Ley 1581 octubre 17 de 2012 Por la cual se dictan disposiciones generales para la

protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
- Ley 594 de 2000 - Ley General de Archivos.
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.
- Ley 527 de 1999 - Ley de Comercio Electrónico.
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos trámites innecesarios existentes en la Administración Pública.
- Ley 57 de 1985 - “Por la cual se ordena la publicidad de los actos y documentos oficiales.”

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:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **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 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 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 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.

- **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 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 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.

- **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.

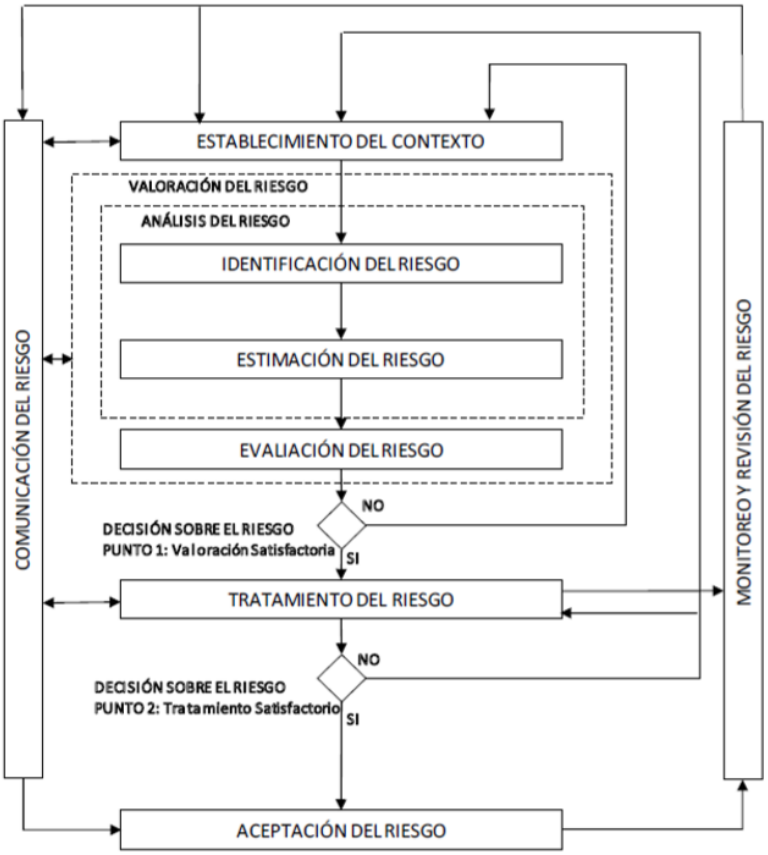


Imagen 2. Tomado de la NTC-ISO/IEC 27005

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; procesos que si llegan a tener alguna modificación afecta la toma de decisiones de la entidad.
- **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 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. (PC, portátiles, servidores, impresoras, documentos en papel, etc.).
- **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.).
- **Sitio:** todos los lugares en los cuales se pueden aplicar los medios de seguridad de la entidad. (oficinas administrativas, consultorios médicos, odontológicos y de enfermería)
- **Estructura organizativa:** responsables, contratistas, áreas etc.

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.
2. **Identificación de Riesgos:** Identificar las causas, riesgo, consecuencias y clasificación del riesgo.
3. **Análisis:** Calificación y evaluación del riesgo.
4. **Valoración:** Identificación y evaluación de controles.
5. **Manejo:** Determinar, las acciones para el fortalecimiento de los controles.
6. **Seguimiento:** Evaluación integral de los riesgos.

1. 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 entre otros.

Esta etapa se centra en determinar las amenazas y debilidades de la ESE Salud del Tundama; es la base para la identificación del riesgo, dado que su análisis suministrará la información sobre las CAUSAS del riesgo.

2. Identificación de riesgos

El propósito de esta etapa permite conocer los potenciales eventos, estén o no bajo el 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**		**Identificación**
Son los medios o circunstancias	**+**	Evento que tendrá un impacto	**+**	Efecto que se puede presentar	**+**	De acuerdo a las características	**=**	Identificación del Riesgo
Descripción a adecuada de los Riesgos								Resultado esperado

Se identifican los riesgos institucionales y por procesos que la organización debe gestionar. Una vez disponemos de un listado de riesgos reales que pueden afectar a nuestra institución, estaremos en disposición de poder realizar la evaluación del impacto que sufrirá la E.S.E. Salud del Tundama en caso de que se materialicen estos riesgos.

Como resultado de esta fase obtendremos:

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

DESCRIPCIÓN DE RIESGOS

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los colaboradores, en la ESE Salud del Tundama se identifican los siguientes riesgos de confidencialidad, integridad, disponibilidad y privacidad de la información que se pueden materializar.

1. Los puntos de red ubicados en cada oficina pueden no ser suficientes y se dispondrá nuevos según se va presentando la necesidad.

2. Algunos cables de energía pueden no estar cerca a los escritorios o no ser suficientes para el total de equipos de cada oficina, podría existir riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el colaborador no alcance a ser guardada.

3. En la institución se podría presentar perdida de la información física y/o digital algunas causas para el riesgo son:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectaría los activos de información y de informática.
- El uso de papel reciclable puede afectar la confidencialidad y privacidad de la información si contiene datos de información personal que debe ser reservada.
- Puede presentarse perdida de información si se comparte los recursos informáticos.
- Puede presentarse perdida de información si es llevada en memorias o discos duros, portátiles personales.
- El uso no controlado de equipos portátiles podría generar pérdida de la información por software maliciosos no detectados.
- La falta de digitalización de los documentos podría exponer a perdidas y daños físicos de información.
- Falta de compromiso en el cuidado de los equipos de cómputo por parte de los colaboradores.

a) Causas del riesgo

Para el tratamiento de los riesgos identificados se establecen las siguientes técnicas que permiten identificar las causas para asociadas las cuales se presentan 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 anticiparse a las posibles causas que ocasiona la materialización de los riesgos en relación a materiales, personas, maquinaria, ambiente, métodos y administración.

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 riesgo mediante la definición de controles y planes de manejo:

Clases de riesgo	Definición
Estratégico	Son los riesgos 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

3. 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 información para establecer el nivel de riesgo.

Se realiza la identificación de causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden dificultar el normal desarrollo de las actividades diarias

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. La primera se entiende la posibilidad de ocurrencia del riesgo; Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

a- Calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

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

Escala para calificar el impacto del riesgo							
Tipos de efecto o impacto		**a) Estratégico**	**b) Operativo**	**c) Financieros**	**d) Cumplimiento**	**e) Tecnología**	**f) Imagen**
INSIGNIFICANTE	El hecho tendría consecuencias o efectos mínimos sobre la ESE.	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida no afecta la operación normal de la ESE.	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	El hecho tendría bajo impacto o efecto sobre la ESE.	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida afecta algunos servicios administrativos de la ESE.	Genera investigaciones disciplinarias, fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	El hecho tendría medianas consecuencias o efectos sobre la ESE.	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del servicio	Afecta varios procesos de la ESE.	Afecta a todos los servidores de la ESE.

MAYOR	El hecho tendría altas consecuencias o efectos sobre la ESE.	Afecta el cumplimiento de las metas de la ESE.	Genera intermitencia en el servicio	La pérdida afecta considerablemente el presupuesto de la ESE.	Genera sanciones	Afecta a toda la entidad	Afecta el sector
CATASTRÓFICO	El hecho tendría desastrosas consecuencias o efectos sobre la ESE.	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la ESE.	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la ESE.	Afecta al Departamento	Afecta al Departamento, Gobierno, Todos los usuarios de la ESE.

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

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.

b- 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.
Para facilitar la calificación y evaluación a los riesgos, a continuación, se presenta la matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

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

4. Valoración de los riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos:

1- **Identificando los controles:** Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

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:** Previo a la valoración del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

5. Manejo de riesgos

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

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

Si la evaluación del riesgo residual, lo ubica en la zona baja no se deben formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema, exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

6. Seguimiento de riesgos

El seguimiento a los riesgos y efectividad de los controles es realizado en el comité institucional de gestión del riesgo, se presentan avances sobre el funcionamiento y manejo de los riesgos en sistemas de información.

PROPUESTA DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Establecer políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- Implementar y socializar las políticas de seguridad y privacidad de la información con el personal de la ESE Salud del Tundama.

PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

- Obtener una nube dedicada para la información de la ESE Salud del Tundama con el fin de tener un respaldo en caso de accidentes referentes a pérdidas de estas.

PLAN DE CONTINUIDAD

- Socializar con los colaboradores de la ESE Salud del Tundama la importancia el Plan de contingencia, para hacer frente a incidentes graves de seguridad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.
- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

  a. Detectar el riesgo
  b. Plantear controles y efectuar las implementaciones respectivas.
  c. Mitigar el riesgo.

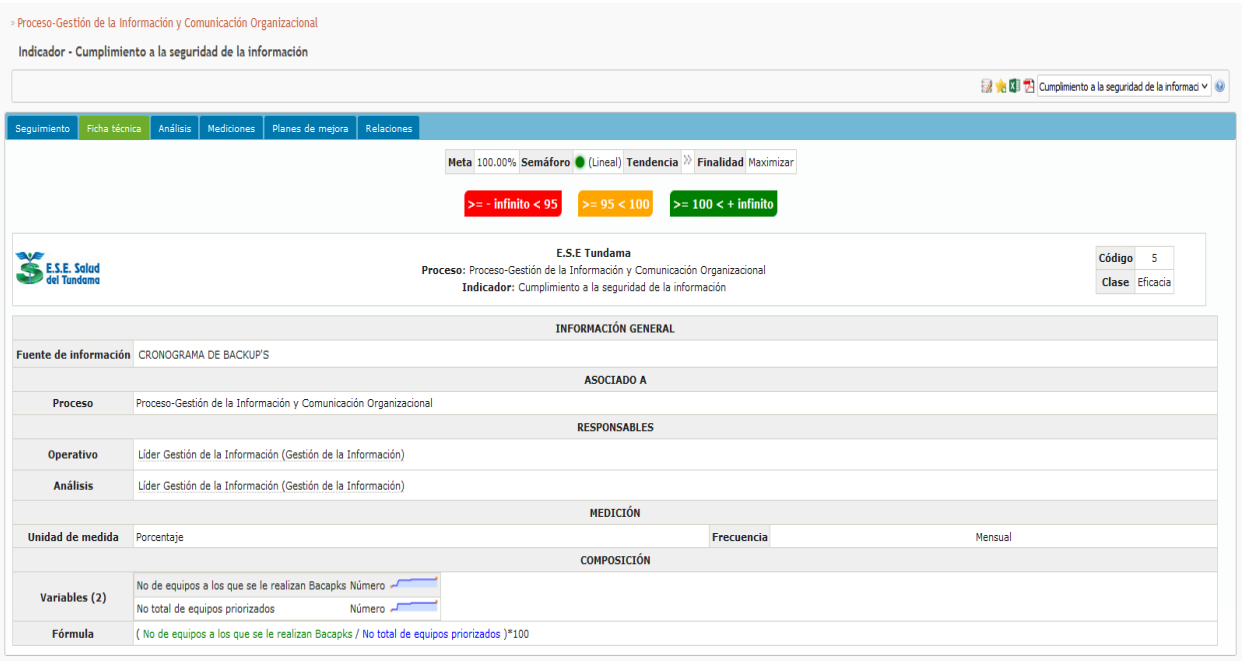
IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

- El análisis permitió identificar que la ESE Salud del Tundama requiere resocializar la política de seguridad y confidencialidad de la información.
- Socialización y capacitación de temas de seguridad informática.
- Ambiente con la seguridad física adecuada.
- Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

INDICADORES

La medición se realiza con un indicador - Cumplimiento a la seguridad de la información, que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, que servirá como insumo para el componente de mejora continúa permitiendo adoptar decisiones de mejora sobre Seguridad de la información.

Fuente: Ficha técnica, Indicador Cumplimiento a la seguridad de la Información.



» Proceso-Gestión de la Información y Comunicación Organizacional

Indicador - Cumplimiento a la seguridad de la información

Cumplimiento a la seguridad de la informaci

Seguimiento | Ficha técnica | Análisis | Mediciones | Planes de mejora | Relaciones

Meta 100.00% Semáforo (Lineal) Tendencia Finalidad Maximizar

>= - infinito < 95 | >= 95 < 100 | >= 100 < + infinito

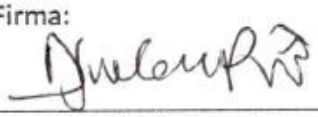
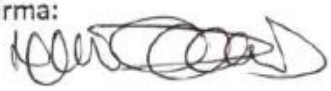
E.S.E. Salud del Tundama

E.S.E Tundama
Proceso: Proceso-Gestión de la Información y Comunicación Organizacional
Indicador: Cumplimiento a la seguridad de la información

Código 5
Clase Eficacia

INFORMACIÓN GENERAL			
Fuente de información	CRONOGRAMA DE BACKUP'S		
ASOCIADO A			
Proceso	Proceso-Gestión de la Información y Comunicación Organizacional		
RESPONSABLES			
Operativo	Líder Gestión de la Información (Gestión de la Información)		
Análisis	Líder Gestión de la Información (Gestión de la Información)		
MEDICIÓN			
Unidad de medida	Porcentaje	Frecuencia	Mensual
COMPOSICIÓN			
Variables (2)	No de equipos a los que se le realizan Bacapks Número No total de equipos priorizados Número		
Fórmula	(No de equipos a los que se le realizan Bacapks / No total de equipos priorizados)*100		

Fuente: Sistema de gestión de calidad Almera.

Elaborado por: Edwin Andrés Romero Agudelo	**Cargo:** Líder Gestión Información	**Fecha:** 23/06/2020
Ultima Actualización: Deicy Jimena Gutiérrez Pérez	**Cargo:** Profesional Apoyo Gestión de Información	**Fecha:** 19/09/2023 **Firma:** 
Revisado por: Nelly Nayibe Dallos Lara	**Cargo:** Líder de Mejoramiento Continuo	**Fecha:** 19/09/2023 **Firma:** 
Aprobado por: Catherine Van Arcken Martínez	**Cargo:** Gerente	**Fecha:** 19/09/2023 **Firma:**