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

TABLA DE CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. CAMPO DE APLICACIÓN 3
4. ACTUALIZACIÓN 3
5. DEFINICIONES 4
6. GENERALIDADES 6
7. METODOLOGIA 8

1. OBJETIVO

Definir y establecer un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la ESE Hospital Geriátrico San Miguel, con el propósito de implementar controles efectivos que reduzcan el impacto de los riesgos sobre la organización. Este plan busca garantizar la protección de la información institucional, fortalecer la confianza en su manejo, y cumplir con los estándares legales y normativos en materia de seguridad de la información.

OBJETIVOS ESPECIFICOS

- Garantizar el cumplimiento de los requisitos legales y reglamentarios aplicables a la legislación colombiana en materia de seguridad y privacidad de la información.
- Identificar, evaluar y gestionar los riesgos relacionados con la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación, asegurando que los controles implementados respondan a los contextos específicos de la Entidad.
- Promover y fortalecer la apropiación del conocimiento en la gestión de riesgos, capacitando al personal de la Entidad en buenas prácticas relacionadas con la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información inicia con la identificación y análisis de los riesgos relacionados con la seguridad de la información dentro de la ESE Hospital Geriátrico San Miguel. Comprende la evaluación de los activos, amenazas, vulnerabilidades e impactos, y culmina con la implementación de controles específicos para mitigar dichos riesgos. Este alcance abarca todos los procesos, servicios, sistemas, activos tecnológicos y recursos humanos vinculados al manejo, protección y continuidad de la información institucional.

3. CAMPO DE APLICACIÓN

Este Plan de Tratamiento de Riesgos aplica a todos los procesos y servicios de la E.S.E. Hospital Geriátrico San Miguel que involucren la gestión, almacenamiento, transmisión y protección de la información institucional. El plan se enfocará especialmente en los riesgos clasificados como de niveles Alto y Extremo, conforme a los lineamientos establecidos por el Ministerio TIC, asegurando que se implementen los controles necesarios para minimizar los impactos potenciales en la organización. Asimismo, incluye tanto los sistemas digitales como los procesos físicos relacionados con la seguridad y privacidad de la información.

4. ACTUALIZACIÓN

El Plan de Tratamiento de Riesgos debe ser revisado y actualizado al menos una vez al año como parte del proceso de mejoramiento continuo de la E.S.E. Hospital Geriátrico San Miguel.

Adicionalmente, deberá ser actualizado en los siguientes casos:

- Cuando se produzcan cambios en la normatividad vigente relacionada con la seguridad y privacidad de la información.
- Si se identifican nuevos riesgos o amenazas que requieran la implementación de controles adicionales.
- Cuando se detecten oportunidades de mejora en la metodología, procesos o herramientas utilizadas para la gestión de riesgos.
- Si ocurren incidentes de seguridad significativos que evidencien la necesidad de ajustes en los controles implementados.

Estas actualizaciones asegurarán la vigencia y eficacia del plan en la protección de la información institucional.

5. DEFINICIONES

Confidencialidad: Se refiere a la capacidad de proteger la información sensible de una organización de ser divulgada a personas no autorizadas. Su incumplimiento puede generar violaciones legales, pérdida de confianza por parte de clientes y proveedores, y daños a la reputación de la empresa. Esto incluye accesos no autorizados, filtraciones y fugas de datos.

Integridad: Es la característica de la información que asegura que esta se mantenga intacta, sin alteraciones no autorizadas. La integridad es fundamental para garantizar la fiabilidad de los datos, ya que cualquier cambio no autorizado puede alterar los procesos de la organización, comprometiendo decisiones y resultados. Un fallo en esta área puede afectar gravemente la operación y seguridad de la empresa.

Disponibilidad: Hace referencia a la capacidad de asegurar que los activos de información estén accesibles y operativos cuando se necesiten. La falta de disponibilidad de estos activos puede causar interrupciones en el servicio, lo que a su vez afectaría la productividad, especialmente en áreas clave de la organización, como operaciones y comunicación.

Activos de la Información: Incluyen todos los recursos que una organización utiliza para operar y que tienen valor, tales como los datos, el software, el hardware, los elementos de redes y comunicaciones, la infraestructura tecnológica y los recursos humanos. La protección de estos activos es esencial para el funcionamiento seguro y eficiente de la organización.

Información: Son los datos que una organización maneja en diferentes formatos (digitales, impresos, etc.). La información es el insumo básico de los procesos empresariales, y su gestión correcta asegura la continuidad y efectividad de las operaciones.

Riesgo: Es la posibilidad de que ocurra un evento que afecte los objetivos organizacionales o el funcionamiento de un proceso. Este evento puede tener consecuencias negativas que desvíen o impidan el cumplimiento de los objetivos de la empresa.

Amenazas: Son cualquier condición o circunstancia que pueda explotar una vulnerabilidad y dañar un activo de información. Las amenazas incluyen ataques cibernéticos, fallos en los sistemas, desastres naturales, errores humanos y otros factores que pueden comprometer la seguridad de los datos y los sistemas.
Vulnerabilidad: Es la debilidad o deficiencia en un sistema, proceso o control de seguridad que puede ser explotada por una amenaza para causar daño. Las vulnerabilidades pueden ser tecnológicas, humanas o de proceso, y su mitigación es crucial para reducir los riesgos asociados.
Impacto: Es la medida del daño que un evento o amenaza puede causar a un activo de información o al funcionamiento de la organización. El impacto puede ser financiero, operativo, legal, o de reputación, y la gravedad depende de la naturaleza del activo afectado y de la magnitud del evento.
Análisis de Riesgos: Es el proceso en el que se identifican y evalúan los riesgos a los que está expuesta la organización. Durante este análisis se determinan los activos críticos y su importancia para la seguridad, se identifican las amenazas y vulnerabilidades, y se asignan probabilidades e impactos a los diferentes eventos de riesgo. Este paso es fundamental en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
Controles: Son medidas implementadas para proteger los activos de información y reducir la probabilidad de ocurrencia de un riesgo. Los controles pueden ser preventivos, correctivos o detectivos y deben ser ajustados según los resultados del análisis de riesgos para ser eficaces en la gestión de la seguridad.
Fuente de Riesgo: Es el origen de un riesgo, es decir, cualquier elemento o factor que, por sí mismo o en combinación con otros, tiene el potencial de generar una amenaza o un evento que cause daño. Las fuentes de riesgo pueden ser internas o externas a la organización.
Gestión de Incidentes de Seguridad de la Información: Consiste en los procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes que afectan la seguridad de la información. Un manejo adecuado de incidentes ayuda a mitigar los efectos de los riesgos y mejora la respuesta ante futuros eventos.
Incertidumbre: Es el estado de desconocimiento sobre la ocurrencia de un evento o la posibilidad de que un riesgo se materialice. La incertidumbre siempre está presente en los procesos de gestión de riesgos, ya que no es posible prever con total certeza qué ocurrirá en el futuro.
Mecanismos de Protección de Datos Personales: Son las alternativas y medidas implementadas para proteger los datos personales de los titulares. Esto incluye controles como el acceso restringido, la anonimización o el cifrado, que ayudan a preservar la privacidad y la seguridad de los datos personales frente a accesos no autorizados o su mal uso.
Nivel de Riesgo: Es una medida que combina la probabilidad de que ocurra un evento dañino y el impacto que tendría este evento en la organización. El nivel de riesgo se calcula generalmente a través de la multiplicación de la probabilidad y el impacto, pero también puede evaluarse utilizando otras metodologías, como matrices de probabilidad e impacto.
Plan de Tratamiento de Riesgos: Es el documento en el que se detallan las acciones que

la organización llevará a cabo para gestionar los riesgos que no son aceptables. Este plan incluye la implementación de controles y la definición de las estrategias necesarias para proteger los activos de información frente a amenazas.

Riesgo de Seguridad de la Información: Es la posibilidad de que una amenaza explote una vulnerabilidad para causar un daño en los activos de información. Este tipo de riesgo se considera una combinación de la probabilidad de un evento y las consecuencias de su materialización.

Tolerancia al Riesgo: Es el umbral o nivel máximo de desviación aceptable respecto al nivel de riesgo que la organización está dispuesta a asumir. Este valor es determinado por la entidad según su apetito de riesgo y su capacidad para gestionar y mitigar los posibles impactos.

Trazabilidad: Es la capacidad de rastrear y asociar de manera inequívoca todas las acciones realizadas sobre la información o un sistema de tratamiento de datos a una persona o entidad responsable. La trazabilidad es crucial para la auditoría, el monitoreo y la mejora continua en la gestión de la seguridad.

6. GENERALIDADES

De acuerdo con la norma ISO 27001, el riesgo se define como la “combinación de la probabilidad de ocurrencia de un evento de seguridad de la información y su consecuente impacto”. Esto puede entenderse como la posibilidad de sufrir daños o pérdidas a consecuencia de un incidente de seguridad. Dentro del contexto de la gestión de riesgos, la amenaza es uno de los componentes clave. Esta puede ser un agente, ya sea humano o no humano, que identifica y explota una vulnerabilidad en un sistema, provocando un resultado inesperado y no deseado.

ROLES Y RESPONSABILIDADES

El éxito en la administración de riesgos depende de la participación activa y comprometida de todos los actores clave dentro de la organización, como la Alta Dirección, servidores públicos y contratistas. A continuación, se detallan los roles y responsabilidades de los involucrados:

Alta Dirección: Tiene la responsabilidad de aprobar las directrices para la administración del riesgo en la entidad. Además, la Alta Dirección debe liderar el fortalecimiento y la implementación de la política de gestión de riesgos, garantizando que todos los niveles de la organización trabajen en conjunto para mitigar los riesgos identificados.

Sistema Integrado de Gestión (SIG): El SIG es responsable de acompañar y supervisar la aplicación de la metodología seleccionada para la gestión de riesgos. Además, coordina, lidera, capacita y asesora en la implementación de la metodología en todos los niveles organizacionales.

Responsables de Procesos y Subprocesos: Son los encargados de identificar, analizar, evaluar y valorar los riesgos de la entidad, tanto a nivel de procesos como institucionales, al menos una vez al año. Aunque los líderes de procesos apoyan la gestión de riesgos, cada responsable de proceso debe garantizar que se definan y gestionen los riesgos

específicos de su área. Deben establecer estrategias para tratar los riesgos, asignar responsabilidades y asegurar que todos los empleados de sus áreas comprendan y gestionen los riesgos asociados a sus actividades diarias.

Servidores Públicos y Contratistas: Tienen la responsabilidad de ejecutar los controles y acciones establecidas para la administración de riesgos. Además, deben aportar en la identificación de riesgos adicionales que puedan afectar la operación de los procesos y la gestión general de la entidad.

Asesor de Control Interno: Debe evaluar y hacer seguimiento a la política de administración de riesgos, así como a los procedimientos y controles implementados para su gestión, asegurando que se cumpla la normativa interna y externa de seguridad. **Equipo de Gestión de Riesgos y de Incidentes de Seguridad de la Información:** Este equipo tiene varias funciones críticas, que incluyen:

- **Detección de Incidentes de Seguridad:** Monitorear y verificar continuamente los sistemas de control para detectar posibles incidentes de seguridad de la información.
- **Atención de Incidentes de Seguridad:** Recibir y gestionar los incidentes de seguridad conforme a los procedimientos establecidos, asegurando que se aborden rápida y eficientemente.
- **Anuncios de Seguridad:** Mantener informados a los empleados, contratistas y terceros sobre nuevas vulnerabilidades, actualizaciones en las plataformas y mejores prácticas de seguridad mediante medios de comunicación internos como la web, intranet o correo electrónico.
- **Auditoría y Trazabilidad de Seguridad Informática:** Realizar verificaciones periódicas sobre el estado de los sistemas para identificar vulnerabilidades emergentes y posibles brechas de seguridad, lo que permite aplicar medidas correctivas a tiempo.
- **Clasificación y Priorización de Servicios Expuestos:** Identificar y clasificar los servicios críticos y las aplicaciones expuestas para su protección y prevenir o mitigar posibles ataques.
- **Investigación y Desarrollo:** Llevar a cabo investigaciones continuas para descubrir nuevas soluciones tecnológicas o el desarrollo de herramientas de protección innovadoras, con el fin de abordar nuevas amenazas y mejorar la seguridad de la información.

Este grupo está conformado por:

- Encargado del proceso Planeación y Calidad o su delegado.
- Líder de Gestión de Talento Humano o su delegado.
- Encargado del proceso en Sistemas de Información. (Líder de grupo)
- Líder del proceso de Control Interno o su delegado.
- Líder del Proceso de Gestión Documental o su delegado.

7. METODOLOGIA

Para llevar a cabo el análisis de riesgos en seguridad informática, se adopta la metodología establecida en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital”, propuesta por el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones. Esta metodología proporciona una base sólida para asegurar que la entidad logre sus objetivos, cumpla con los requisitos legales y reglamentarios, y proteja adecuadamente los recursos del Estado.

Al aplicar esta metodología, se busca cumplir con las normativas vigentes, identificar y gestionar los riesgos de manera efectiva en todos los niveles de la entidad, y establecer controles adecuados para mitigar dichos riesgos.

La gestión del riesgo implica la implementación de un conjunto de elementos de control y sus interrelaciones, con el fin de que la institución pueda evaluar e intervenir en aquellos eventos, tanto internos como externos, que puedan tener un impacto positivo o negativo en el logro de los objetivos institucionales. La gestión del riesgo, además de contribuir a la consolidación del Sistema de Control Interno, fomenta una cultura de autocontrol y autoevaluación dentro de la organización.

De acuerdo con lo establecido en la guía, la gestión del riesgo permite a la institución identificar áreas críticas que requieren atención especial, asegurando que se tomen medidas preventivas y correctivas ante las amenazas y vulnerabilidades detectadas. Para la correcta gestión de riesgos en Seguridad Digital, se deben realizar las siguientes actividades:

DESCRIPCIÓN

Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Mejoramiento	Identificación de oportunidad de mejora y diseño de controles en la matriz de riesgo	Equipo de Gestión de riesgos e incidentes de seguridad de la información	Marzo 2025	Mayo 2025
Monitoreo y revisión	Generación, presentación y reporte de riesgos identificados durante el año en curso	Encargado del proceso en Sistemas de Información	Mayo 2025	Diciembre 2025
	Verificación del cumplimiento de los controles definidos en la matriz de riesgos	Equipo de Gestión de riesgos e incidentes de seguridad de la información	Marzo 2025	Diciembre 2025
Comunicación	Presentación a Comité de Gestión y Desempeño de avances en el cumplimiento de controles definidos en la matriz de riesgos	Encargado del proceso en Sistemas de Información	Abril 2025	Diciembre 2025
	Publicación de seguimiento a matriz de riesgos	Encargado del proceso en Sistemas de Información	Junio 2025	Junio 2025

La implementación de estas actividades contribuirá a que la entidad esté mejor preparada para enfrentar los riesgos en seguridad digital y cumpla con los estándares establecidos para la protección de la información.

San Miguel E.S.E. HOSPITAL GERIÁTRICO

Control de Emisión		
Elaborado por: ORIGINAL FIRMADO	Revisado por: ORIGINAL FIRMADO	Aprobado por: ORIGINAL FIRMADO
Ruben Dario Mina Campaz Cargo Sistemas e Informacion	Idaline Diaz Escobar Cargo Calidad -Asosindisalud	Oscar Eduardo Erazo Castro Cargo Subgerente Administrativo y Financiero
Fecha: 26-01-2026	**Fecha:** 26-01-2026	**Fecha:** 26-01-2026

Cambios de Versión				
No.	**Versión**	**Descripción del cambio**	**Responsable**	**Fecha de actualización**
1	1	Creación del documento	Proceso de Sistemas	26/01/2026