Hospital Regional de Sogamoso E.S.E.

Plan de servicio y/o proceso: PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACIÓN

Hospital Regional de Sogamoso E.S.E.	**Hospital Regional de Sogamoso E.S.E.** **Proceso**: Gestión de la información **Subproceso**: Gestión de la información **Plan de servicio y/o proceso**: PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFOMACIÓN	**Código** A-GI-GI-PS-02 **Fecha** 2025-01-31 **Versión** 1

Estratégico	Misional	Apoyo	Evaluación y control

RESPONSABLE

Líder Gestión de la Información (Gestión de la Información)

OBJETIVO GENERAL

Establecer un plan de tratamiento de riesgos de seguridad y privacidad de la información en el Hospital Regional de Sogamoso que garantice la protección de los activos de información, promueva una cultura de seguridad en el personal y asegure la alineación de las tecnologías de la información con los objetivos estratégicos de la institución.

OBJETIVOS ESPECIFICOS

- Estructurar y consolidar un plan de tratamiento de riesgos de seguridad y privacidad de la información
- Reconocer el inventario de activos de información, para gestionar los riesgos de seguridad y privacidad de la información de acuerdo con las políticas y manuales adoptados por el Hospital Regional de Sogamoso.
- Generar estrategias para fortalecer la cultura de protección de la información dentro del personal.
- Establecer y aplicar de manera permanente el plan de tratamiento de riesgos a todos los activos de información de la entidad.

ALCANCE

Para el Hospital Regional Sogamoso E.S.E, la estructuración y puesta en marcha de un Plan de tratamiento de riesgos de Seguridad y privacidad de la Información tiene un carácter vinculante para todas las dependencias y recursos humanos de la entidad. Aplica a la totalidad de procesos institucionales, activos y componentes de la información.

RESPONSABLES

- **Responsables del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información:**

1. **Línea Estratégica: Alta Dirección (Junta Directiva y gerencia),** Encargado de analizar los riesgos, amenazas institucionales y bridar los recursos necesarios para iniciar el tratamiento de los riesgos, así como de asegurar la aplicación de las políticas y medidas de seguridad en su área.
2. **Primera línea de defensa:** lideres de proceso y equipos de trabajo encargados de apoyar la Identificación y valoración de cada activo de información en cada proceso donde aplique la gestión del riesgo de seguridad y privacidad de la información
3. **Responsable de Seguridad de la Información:** Persona designada para coordinar y gestionar la implementación del plan. Se encarga de asegurar que todas las medidas y políticas se apliquen correctamente y que se realicen revisiones periódicas del plan.
4. **Equipo de TI y Seguridad:** Equipo técnico encargado de implementar los controles y medidas de seguridad necesarios para proteger los activos de información. También se ocupa de monitorear las amenazas y responder a incidentes de seguridad.
5. **Todo el Personal del Hospital:** Todos los empleados, contratistas y colaboradores tienen la responsabilidad de cumplir con las políticas y procedimientos establecidos en el plan de tratamiento de riesgos. La formación

y concienciación en seguridad de la información son claves para asegurar su participación.

6. **Proveedor de Servicios Externos:** En caso de que el hospital cuente con servicios de terceros para la gestión de la seguridad de la información, estos proveedores también tienen responsabilidades específicas en el tratamiento del riesgo.

MARCO LEGAL Y/O TEÓRICO

NORMA	DESCRIPCION
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).
Decreto 1078 de 2015	Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
DECREETO 1008 DE 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015.
	Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Guía para administración del riesgo y el diseño de controles en entidades públicas – Versión 6	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2022

DEFINICIONES

Activo de Información: Cualquier dato, sistema, hardware o recurso que tenga valor para la organización y necesite ser protegido.

Amenaza: Cualquier circunstancia o evento con el potencial de dañar la información o los sistemas de información.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información por la cual se asegura que solo las personas autorizadas pueden acceder a ella.

Control: Medida establecida para reducir la probabilidad o el impacto de un riesgo. Puede ser de naturaleza

preventiva, correctiva o de detección.

Cumplimiento: Adherencia a las leyes, regulaciones y políticas aplicables a la gestión de seguridad y privacidad de la información.

DAFP: Departamento administración de la función publica

Disponibilidad: Propiedad de la información por la cual se asegura que las personas autorizadas tienen acceso a la información y a sus recursos asociados cuando lo necesiten.

Identificación del Riesgo: Proceso para determinar lo que puede suceder, por qué y cómo. Puede hacerse a cualquier nivel: total, por áreas, por procesos, incluso, bajo el viejo paradigma, por funciones; desde el nivel estratégico hasta el más sencillo operativo.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de la información por la cual se asegura que la información es exacta, completa y se mantiene sin alteraciones no autorizadas.

Gestión de Incidentes: Proceso de identificación, análisis, y respuesta a incidentes de seguridad de la información para minimizar su impacto.

Riesgo: La posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo en los activos de información de la organización.

Plan de Continuidad del Negocio: Conjunto de procedimientos y recursos predefinidos para asegurar la continuidad de las operaciones críticas de la organización en caso de una interrupción significativa.

Política: Conjunto de principios o reglas establecidas por una organización para guiar sus acciones y decisiones en un área específica, en este caso, la seguridad de la información.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Usuario: Persona autorizada que utiliza los sistemas y recursos de información de la organización.

Vulnerabilidad: Una debilidad en los sistemas, procesos o controles que puede ser explotada por una amenaza.

DIAGNÓSTICO Y/O SITUACIÓN ACTUAL

El Hospital Regional de Sogamoso ha implementado recientemente un nuevo mapa de procesos, lo que implica una reestructuración en la forma en que se gestiona la información y se prestan los servicios. Esta modificación exige la elaboración de un nuevo plan de riesgos de seguridad y privacidad de la información, así como la actualización de la matriz de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de los datos en este nuevo contexto. El análisis de riesgos deberá considerar los cambios en los flujos de información, las nuevas responsabilidades y los posibles puntos débiles generados por la reorganización, con el fin de garantizar la protección de la información sensible de pacientes y la institución en el marco del nuevo mapa de procesos.

RECURSOS, MATERIALES, INSUMOS Y EQUIPOS

1. Recursos Humanos:

- **Profesional en Seguridad de la Información:** Profesional con experiencia en gestión de riesgos y seguridad informática.
- **Lideres de cada proceso:** Personas designadas para asegurar la implementación del plan en sus respectivas áreas.
- **Personal de TI:** Equipo técnico encargado de la implementación y mantenimiento de los controles de seguridad

2.Materiales y Documentación:

- Políticas, Procedimientos, Normas internas y externa: Instrucciones claras y detalladas sobre cómo gestionar y mitigar riesgos.
    - **PROGRAMA DE GESTION DEL RIESO**
    - **GUIA PARA LA ADMINISTRACION DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PUBLICAS:** RIEGO DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL, FUNCION PUBLICA 2022 versión 6
    - **ANEXO 4:** LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PUBLICAS, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
    - **Política de seguridad y privacidad de la información:** Resolución 358 del 19 de octubre del 2021 "por medio de la cual se adopta la POLITICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACION del HOSPITALREGIONAL DE SOGAMOSO E.S.E"
    - **Política de tratamiento de datos personales:** Resolución 033 del 23 de enero del 2019 "por medio de la cual se establece las políticas de tratamiento de datos personales del HOSPITAL REGIONAL DE SOGAMOSO ESE"
    - **Manuales y Guías de Seguridad:** Material de referencia para el personal del hospital.

3. Insumos

- **Herramientas de Monitoreo y Detección:** Software que permita la supervisión continua y la detección de amenazas.

Suricata:

Suricata es una herramienta de detección y prevención de intrusiones (IDS/IPS) de código abierto, diseñada para proporcionar una defensa robusta y proactiva contra amenazas en la red. Esta solución se instalará en el servidor asignado a la seguridad perimetral, donde desempeñará un papel crucial en la protección de los activos de información de la organización. Suricata es capaz de examinar el tráfico de red en tiempo real, identificando patrones maliciosos y comportamientos anómalos que podrían indicar intentos de intrusión. Su arquitectura permite el análisis profundo de paquetes, lo que facilita la detección de amenazas sofisticadas y la respuesta inmediata a incidentes de seguridad. Además, Suricata soporta múltiples protocolos y puede integrarse con otras herramientas de seguridad, lo que la convierte en una opción versátil para entornos de red complejos. Una de las características destacadas de Suricata es su capacidad para personalizar reglas de detección, lo que permite a los administradores adaptar la herramienta a las necesidades específicas de seguridad de la organización. Esto incluye la posibilidad de definir reglas que se alineen con las políticas de seguridad y los riesgos identificados en el entorno. Al implementar Suricata en el servidor de seguridad perimetral, la organización podrá mejorar significativamente su postura de seguridad, monitoreando y protegiendo su infraestructura contra una amplia gama de amenazas cibernéticas. Esto no solo ayuda a prevenir intrusiones, sino que también proporciona visibilidad sobre el tráfico de red, permitiendo una mejor gestión de incidentes y una respuesta más rápida ante posibles ataques.

Sistemas de Backup y Recuperación: Soluciones para asegurar la continuidad del negocio y la recuperación ante desastres.

Las copias de seguridad son almacenadas en lugares diferentes para garantizar la integridad de la información

- Servidor Principal centro de Datos Hospital Regional de Sogamoso E.S.E: La ubicación de las copias de seguridad de la base de datos del sistema de información hospitalario, permanecen en el servidor principal en las carpeta redireccionada y configurada por el administrador del sistema de información.
- Discos Duros Externos: Las copias de seguridad son extraídas del servidor principal y son almacenadas en discos duros externos que permanecen en custodia del líder del proceso en la oficina de Gestión de la información.
- Copias de seguridad Cloud: El Hospital Regional de Sogamoso ESE cuenta con un sistema de almacenamiento externo (Cloud) en el cual se almacenan las copias de seguridad extraída del servidor en producción.

4. Equipos y tecnología

- **Servidores:** Para almacenar y procesar información de forma segura.
- **Dispositivos de Seguridad de Red:** Firewalls, sistemas de detección y prevención de intrusiones, y otros equipos de seguridad de red.
- **Sistemas de Autenticación y Control de Acceso:** Herramientas que aseguren que solo personas

autorizadas puedan acceder a la información crítica.
- **Equipos de Comunicación Segura:** Dispositivos que aseguren la privacidad y seguridad de las comunicaciones internas y externas.

5. Infraestructura Física:

- **Centros de Datos:** Instalaciones con medidas físicas de seguridad para proteger los equipos de TI.
- **Ambientes Controlados:** Espacios donde se maneje información sensible con acceso restringido.

6. Capacitaciones y formación

- **Programas de Concienciación:** Iniciativas para educar al personal sobre la importancia de la seguridad de la información y la privacidad.
- **Cursos y Talleres:** Formación continua para mantener al personal al día con las mejores prácticas y nuevas amenazas.

DESARROLLO DEL DOCUMENTO

1. Metodología plan tratamiento de riesgos de seguridad de la información

Desarrollo del cronograma o metodología

Para la identificación de los riesgos de seguridad y privacidad de la información se deben tener en cuenta los diferentes aspectos con los que cuenta la institución la infraestructura física, las diferentes áreas que contemplan el mapa de procesos de la entidad, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos con los que cuenta y reconocer los posibles riesgos a los cuales expone la institución, para lo cual es necesario seguir la metodología:

- **Planeación Gestión del riesgo:** Definición de metodología y estrategias aplicar para realizar la correcta estructuración de la planeación del riesgo en la entidad, Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad, de su correcto análisis, se pueden inferir las causas del riesgo.
- **Identificación de activos:** esta etapa está dirigida a identificar, clasificar y valorar todos a los activos de información de la organización. dónde están?, ¿tipo de información? estado, responsables, medios físicos, magnéticos en la nube, etc.

Los activos de la información se pueden clasificar en primarios y de soporte, para los primeros se identifican los siguientes:

Procesos: Cuya perdida imposibilita el cumplimiento de la misión institucional, procesos claves para el logro de requisitos legales o contractuales.

Información: Activo vital para la ejecución de la actividad, puede involucrar características de tipo confidencial, estratégica o de alto costo para la organización

Actividades y procesos: Si se degradan o adquieren vicios, imposibilitan el cumplimiento de los objetivos

Para la clasificación de soporte se tiene:

Hardware: Elementos físicos que dan soporte a los procesos

Software: Todas aquellas herramientas, programas, aplicaciones que dan soporte a procesos dentro de una entidad.

Redes: Dispositivos de las telecomunicaciones que permiten interconectar dispositivos electrónicos.

Personal: Gestión humana involucrada en los sistemas de información

2. Ciclo general del riesgo

El ciclo general de los riesgos en la Institución determinado desde su política de administración del riesgo será trazado por la metodología impartida por el Departamento Administrativo de la Función Pública, donde se reúnen las etapas de identificación, valoración, definición de controles, monitoreo y seguimiento, para todas las tipologías de de riesgo, como se detalla a continuación:

Ilustración 1. Proceso para la administración del riesgo en seguridad de la información

Fuente: E-DO-GR-PG-01 PROGRAMA DE GESTIÓN DEL RIESGO

2.1. Descripción del riesgo: permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías

Tabla 2. Clasificación de riesgos en Metodología DAFP, complementada con tipologías

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: / Adoptado Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP, Versión 6, 2022.

Teniendo en cuanta la tabla anterior se definieron una serie de factores generadores del riesgo, para poder definir la clasificación de los riesgos su interrelación es la siguiente

Ilustración 3 Relación ente factores de riesgo y clasificación del riesgo

Fuente: / Adoptado Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP, Versión 6, 2022.

2.2. Valoración del riesgo

Esta evaluación del riesgo se realiza de manera cualitativa generando una comparación entre la probabilidad del riesgo vs el impacto del mismo.

- ***Probabilidad***

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, determina con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado. Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que

se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 4 se establecen los criterios para definir el nivel de probabilidad.

Ilustración 4 Relación ente factores de riesgo y clasificación del riesgo

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: / Adoptado Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP, Versión 6, 2022.

- **Impacto**

Teniendo en cuenta que la Guía de administración del riesgo adoptada en 2018, se pueden identificar dentro del impacto: afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto de los impactos aplicables a cada tipología.

Considerando la metodología adoptada se definen los criterios para establecer el nivel de impacto por afectación económica y frente al reputacional se adoptan de acuerdo a la Guía del DAFP.

Tabla 3. Criterios para definir el nivel de impacto

Nivel	Afectación económica	Reputacional
Leve 20%	Afectación menor a 5% presupuesto anual aprobado	El riesgo afecta la imagen del área de la organización.
Menor 40%	Afectación menor a 10% presupuesto anual aprobado	El riesgo afecta la imagen de la entidad internamente, de conocimiento generar interno, Junta Directiva.
Moderado 60%	Afectación menor a 20% presupuesto anual aprobado	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de sus objetivos
Mayor 80%	Afectación menor a 40% presupuesto anual aprobado	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel del sector, departamento o municipio.
Catastrófico 100%	Afectación menor a 60% presupuesto anual aprobado	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel nacional del sector, país.

Fuente: Acuerdo de Junta Directiva No. 012 de 2024, Política y Sistema Integrado de Gestión del Riesgo en el Hospital Regional de Sogamoso.

A partir del análisis de la probabilidad de ocurrencia del Descripción del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor: Bajo, Moderado, Alto y Extremo.

3. Amenazas y Vulnerabilidades a la Seguridad y privacidad de la información

Es la etapa que permite conocer los eventos potenciales, internos o externos que ponen en riesgo el logro de la misión, estableciendo las causas y consecuencias de la ocurrencia del riesgo.

A continuación, se describen una serie de amenazas y vulnerabilidades para el análisis del riesgo:

- **Amenazas comunes:**

D= Deliberadas, A= Accidentales, E= Ambientales

Tabla 4. Amenazas comunes frente a la seguridad y privacidad de la información

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E

TIPO	AMENAZA	ORIGEN
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A, D
	Perdida de suministro de energía	A, D, E
Perturbación debida a la radiación	Falla en equipo de telecomunicaciones	A, D
	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Fallas del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información.	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Fuente: Guía de gestión del riesgo – MinTic

- **Amenazas Humanas**

Tabla 5. Amenazas humanas frente a la seguridad y privacidad de la información

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado

Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información • reservada • Uso inadecuado del • computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o • corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

Fuente: Guía de gestión del riesgo – MinTic

- **Vulnerabilidades**

Tabla 6. Vulnerabilidades frente a la seguridad y privacidad de la información

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS

HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del Equipo

RED	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	

ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de	Abuso de los derechos
	administradores y operadores	
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso

	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	*Uso no autorizado de equipo*
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	*Uso de software falsificado o copiado*
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

Fuente: Guía de gestión del riesgo – MinTic

- Determinación del riesgo: La determinación 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. En este punto es importante destacar que se pueden tener en cuenta algunos criterios para evaluar el riesgo de seguridad.

1. Criticidad de los activos
2. Requisitos legales y reglamentarios
3. Disponibilidad, integridad y confidencialidad
4. El buen nombre de la institución

4. Lineamientos Internos para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

- **Socializados y Apropiados:** Es crucial que todos los funcionarios, contratistas y demás personal del hospital comprendan y adopten los lineamientos del plan debido a su carácter vinculante. Este proceso incluirá talleres, sesiones de capacitación y materiales de apoyo para asegurar la comprensión y el cumplimiento de las políticas.
- **Aplicables a Todos los Procesos:** Los lineamientos deben ser aplicables a todos los procesos estratégicos, misionales y de apoyo del hospital. Esto asegura que todas las áreas y niveles del hospital estén alineados con las políticas de seguridad de la información, promoviendo una cultura organizacional coherente y robusta en términos de seguridad y privacidad de la información.
- **Revisados y Actualizados:** Establecer un proceso de revisión y actualización periódica del plan para que siempre esté alineado con las últimas normativas y tecnologías disponibles, así como con los nuevos riesgos emergentes.
- **Monitoreo y Evaluación:** Implementar mecanismos de monitoreo y evaluación continua para garantizar la eficacia del plan y la adherencia de todos los miembros de la organización a los lineamientos establecidos.

5. Cronograma de actividades plan tratamiento de riesgos de seguridad de la información

Tabla 6. Cronograma actividades plan tratamiento de riesgos de seguridad de la información

Actividad	Responsable	Fecha Inicio	Fecha Terminación
Revisar y ajustar metodología para la gestión de Riesgo de seguridad y privacidad de la información	Líder Gestión de la información Referente de seguridad digital	01/Feb/2025	28/ Feb /2025
Actualizar la política de protección de datos del HRS	Líder Gestión de la información Referente de seguridad digital	01/Mar/2025	28/ Mar /2025
Actualizar los activos de información de la entidad	Líder Gestión de la información Referente de seguridad digital Líder gestión documental	01/ Feb /2025	30/Abr/2025
Actualizar la clasificación de los activos de información de acuerdo con los pilares de la seguridad de la información integridad, confidencialidad y disponibilidad	Líder Gestión de la información Líder gestión documental Lideres de los diferentes procesos	01/May/2025	30/Jun/2025
Construcción de la matriz de riesgos seguridad y privacidad de la información	Líder Gestión de la información Líder gestión de gestión documental Lideres de los diferentes procesos	01/Jul/2025	30/Sep/2025
Realizar el monitoreo a los riesgos de seguridad y privacidad de la información	Líder Gestión de la información	01/ Jul /2025	30/Nov/2025

BIBLIOGRAFÍA

Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Versión 6. 2024.