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

HOSPITAL
SAN JOSÉ DEL GUAVIARE
EMPRESA SOCIAL DEL ESTADO

2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVOS 4
3. ALCANCES 4
4. Limitaciones 5
5. EJECUCIÓN DEL PLAN 5
Debido al constante avance en el manejo de la información digital, se vuelve esencial salvaguardar, proteger y custodiar adecuadamente los activos de la información en la E.S.E Hospital San José del Guaviare. 5
6. ANÁLISIS DEL RIESGO INHERENTE 17
7. IDENTIFICACIÓN DE CONTROLES Y PLAN DE TRATAMIENTO DE RIESGOS. 25
8. Bibliografía 30

1. INTRODUCCIÓN

Considerando que el constante avance de las tecnologías de comunicación y la gestión de la información digital trae consigo nuevos desafíos y amenazas para asegurar la confidencialidad, integridad y disponibilidad de la información generada en los procesos de la E.S.E Hospital San José del Guaviare, resulta fundamental la implementación de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Este plan tiene como objetivo proteger la información frente a eventos que puedan comprometer su integridad, mediante la identificación de los activos de información y la evaluación de sus posibles amenazas y vulnerabilidades, estableciendo controles apropiados para su manejo, basados en el análisis del impacto y la probabilidad de ocurrencia de dichos eventos

2. OBJETIVOS

- Desarrollar el Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información que permita minimizar los riesgos de perdida de activos de la información en la E.S.E Hospital San José del Guaviare.

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.

- Priorizar los riesgos según los criterios establecidos en el Mapa de Riesgos de Seguridad Digital.

- Realizar la identificación de los principales Activos de Información presentes en la E.S.E.

- Identificar las principales amenazas que afectan a los activos.

- Definir el impacto de la ocurrencia de las amenazas.

- Establecer controles, responsables y periodos de ejecución de las acciones de mitigación de las amenazas de los activos de la información.

- Medir a través de indicadores, el manejo de los riesgos establecidos.

3. ALCANCES

Con el fin de llevar a cabo una gestión eficaz de los riesgos de Seguridad y Privacidad de la Información, la E.S.E Hospital San José del Guaviare debe asegurar el compromiso necesario para implementar este plan en todos los procesos institucionales. Esto se logrará mediante la aplicación de buenas prácticas y lineamientos tanto nacionales como locales, buscando que su implementación contribuya a una toma de decisiones informada y a la prevención de incidentes que puedan poner en riesgo los activos de información. Para ello, se designarán roles de liderazgo que brinden apoyo y orientación en la ejecución del Plan, además de capacitar al personal de la Entidad para garantizar su correcta implementación.

4. LIMITACIONES

No asignar los recursos necesarios en el presupuesto para apoyar la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la E.S.E Hospital San José del Guaviare.

5. EJECUCIÓN DEL PLAN

5.1. IMPORTANCIA DE LA GESTIÓN DE RIESGOS

DEBIDO AL CONSTANTE AVANCE EN EL MANEJO DE LA INFORMACIÓN DIGITAL, SE VUELVE ESENCIAL SALVAGUARDAR, PROTEGER Y CUSTODIAR ADECUADAMENTE LOS ACTIVOS DE LA INFORMACIÓN EN LA E.S.E HOSPITAL SAN JOSÉ DEL GUAVIARE.

Figura 1. Proceso de Administración del Riesgo

En línea con los lineamientos establecidos por el Gobierno Nacional, en cumplimiento de la Ley de Transparencia 1712 de 2014 y el programa Gobierno en Línea, que promueven

acciones dentro de las entidades públicas para adaptarse a modelos y estándares que aseguren la protección de la información, como el concurso Máxima Velocidad impulsado por el Ministerio de las TIC, la E.S.E Hospital San José del Guaviare cumple con el Decreto 1078 de 2015, mediante el cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Para la elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se emplearon la Guía 7 sobre Gestión de Riesgos y la Guía 8 referente a los Controles de Seguridad de la Información.

5.2. DEFINICIÓN GESTIÓN DEL RIESGO.

De acuerdo con la Organización Internacional de Normalización (ISO), la gestión del riesgo se entiende como: "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo" (NTC ISO 31000:2011). Por su parte, la Cartilla de Administración de Riesgos del DAFP establece que la gestión del riesgo se divide en los siguientes procesos:

IDENTIFICACIÓN DEL RIESGO

- **Riesgo Estratégico**: Está relacionado con la forma en que se gestiona la Entidad. El manejo de este riesgo se enfoca en aspectos globales vinculados a la misión y al cumplimiento de los objetivos estratégicos, así como a la definición clara de políticas, diseño y conceptualización de la entidad por parte de la alta Gerencia.
  "El Hospital a su servicio"
- **Riesgos de Imagen**: Se refieren a la percepción y confianza que la ciudadanía tiene hacia la institución.
- **Riesgos Operativos**: Involucran los riesgos derivados del funcionamiento y la operatividad de los sistemas de información institucional, la definición de procesos, la estructura de la entidad y la interacción entre sus dependencias.
- **Riesgos Financieros**: Se relacionan con la gestión de los recursos de la entidad, incluyendo la ejecución presupuestal, la elaboración de estados financieros, los pagos, la gestión de excedentes de tesorería y el manejo de bienes.
- **Riesgos de Cumplimiento**: Están vinculados con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, éticos y su compromiso con la comunidad según su misión.
- **Riesgos de Tecnología**: Se refieren a la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras, y al cumplimiento de su misión.

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

El Mapa de Riesgos de Seguridad Digital, proporcionado por el Ministerio de las TIC, define los siguientes tipos de activos de información:

- **Información y Datos de la Entidad**: Son los datos e información almacenada o procesada de manera física o electrónica, tales como bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **Sistemas de Información y Aplicaciones de Software**: Incluyen el software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- **Dispositivos de Tecnologías de Información - Hardware**: Equipos de cómputo que, debido a su criticidad, se consideran activos de información, no solo activos fijos.
- **Soporte para el Saneamiento de Información**: Equipos utilizados para el almacenamiento de información, tales como USB, discos duros, CDs, NAS, entre otros.
- **Servicios**: Servicios de computación y comunicaciones, como internet, páginas de consulta, directorios compartidos e intranet.

Teniendo en cuenta los criterios mencionados, se identifican los siguientes activos de información:

Tipo de activo de información	Activo de información
Información y Datos de la Entidad	• **Registros médicos de pacientes**: Historia clínica, diagnósticos, tratamientos, resultados de laboratorio, imágenes médicas (radiografías, resonancias, etc.). • **Datos administrativos**: Información sobre personal, nóminas, Información sobre ingresos, egresos, presupuestos, y

	reportes financieros, datos sobre cuentas por cobrar, pagos pendientes, historial de pagos de pacientes y aseguradoras, facturas emitidas a pacientes, aseguradoras o terceros, incluyendo detalles de servicios prestados, costos y pagos recibidos, información sobre acuerdos contractuales relacionados con seguros médicos, servicios externos, y acuerdos comerciales. • **Documentos legales y contratos**: Contratos con proveedores, acuerdos de confidencialidad, licencias de software. • **Planes de continuidad del negocio**: Procedimientos de recuperación ante desastres, planes de contingencia. • **Políticas y procedimientos internos**: Manuales de usuario, procedimientos operativos, políticas.
Sistemas de Información y Aplicaciones de Software	• **Sistema de Gestión Hospitalaria**: Software de administración que maneja citas, registros médicos, inventarios, facturación, información financiera, etc (Dinámica Gerencial). • **Sistema de Información Radiológica (PACS)**: Para el manejo de imágenes médicas y la integración con otros sistemas de diagnóstico. • **Software de mantenimiento**: Herramientas que ayudan a mantener el funcionamiento óptimo

	de los equipos informáticos, biomédicos e industriales, gestionando las reparaciones, mantenimiento preventivo, historial de mantenimiento y calibración de los dispositivos.
Dispositivos de Tecnologías de Información - Hardware	• **Servidores**: Servidores que alojan bases de datos críticas (por ejemplo, servidor del software Dinámica Gerencial). • **Estaciones de trabajo**: Computadoras de escritorio o portátiles que utiliza el personal asistencial y administrativo. • **Dispositivos de red**: Routers, switches, firewalls, que aseguran la conectividad y seguridad en la red interna del hospital.
Soporte para el Saneamiento de Información	• **Dispositivos de almacenamiento**: Discos duros internos y externos. • **Almacenamiento en la nube**: Plataformas en la nube utilizadas para guardar datos y hacer backups remotos de la información de la entidad (Drive del correo electrónico institucional). • **Dispositivos de backup**: Unidades de almacenamiento NAS (Network Attached Storage) que guardan copias de seguridad de datos críticos de las estaciones de trabajo principales y bases de datos de los servidores. La entidad cuenta con 2 de estos dispositivos.
Servicios	• Servicio de internet para acceder a plataformas externas.

IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de ocasionar daños a la información, los procesos y los sistemas, y por ende, a la E.S.E Hospital San José del Guaviare. Las amenazas pueden originarse de manera natural o humana, y pueden ser tanto accidentales como deliberadas. Es recomendable identificar todos los posibles orígenes de amenazas, tanto accidentales como deliberadas. Las amenazas deben ser clasificadas de manera general y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas, etc.). A continuación, se presentan las amenazas identificadas:

Activo de información	AMENAZAS
• **Registros médicos de pacientes**: Historia clínica, diagnósticos, tratamientos, resultados de laboratorio, imágenes médicas (radiografías, resonancias, etc.). • **Datos administrativos**: Información sobre personal, nóminas, Información sobre ingresos, egresos, presupuestos, y reportes financieros, datos sobre cuentas por cobrar, pagos pendientes, historial de pagos de pacientes y aseguradoras, facturas emitidas a pacientes, aseguradoras o terceros, incluyendo detalles de servicios prestados, costos y pagos recibidos, información sobre acuerdos contractuales relacionados con seguros médicos, servicios externos, y acuerdos comerciales. • **Documentos legales y contratos**: Contratos con proveedores, acuerdos de confidencialidad, licencias de software.	• **Acceso no autorizado**: Personal no autorizado podría acceder a registros médicos de pacientes. • **Robo o filtración de datos**: Los registros médicos podrían ser robados o filtrados por un ciberataque, comprometiendo la privacidad de los pacientes. • **Ransomware**: Secuestro de los datos por parte de atacantes, pidiendo un rescate para liberarlos. • **Destrucción de datos**: Pérdida de información médica clave debido a fallos en los sistemas o un ataque malicioso. • **Desastres naturales o fallos de infraestructura**: Desastres físicos como incendios o inundaciones que dañan las instalaciones o sistemas.

• **Planes de continuidad del negocio**: Procedimientos de recuperación ante desastres, planes de contingencia. • **Políticas y procedimientos internos**: Manuales de usuario, procedimientos operativos, políticas.	
• **Sistema de Gestión Hospitalaria**: Software de administración que maneja citas, registros médicos, inventarios, facturación, información financiera, etc (Dinámica Gerencial). • **Sistema de Información Radiológica (PACS)**: Para el manejo de imágenes médicas y la integración con otros sistemas de diagnóstico. • **Software de mantenimiento**: Herramientas que ayudan a mantener el funcionamiento óptimo de los equipos informáticos, biomédicos e industriales, gestionando las reparaciones, mantenimiento preventivo, historial de mantenimiento y calibración de los dispositivos.	• **Fallos en el sistema**: Caídas del sistema que pueden interrumpir las operaciones hospitalarias (citas, registros médicos, suministros, etc.). • **Ransomware**: Secuestro del sistema que afecta la disponibilidad de servicios clave (facturación, gestión de pacientes). • **Acceso no autorizado**: Acceso no autorizado por parte de personal malintencionado o cibercriminales. • **Integridad de los datos**: Manipulación o alteración de datos relacionados con los pacientes o la facturación. • **Robo de imágenes médicas**: Filtración de imágenes sensibles de los pacientes (radiografías, resonancias). • **Interrupción del servicio**: Caídas del sistema que dificultan la consulta o diagnóstico a tiempo de las imágenes médicas.
• **Servidores**: Servidores que alojan bases de datos críticas (por ejemplo, servidor del software Dinámica Gerencial). • **Estaciones de trabajo**: Computadoras de escritorio o	• **Ataques DDoS**: Sobrecarga de servidores o redes que interrumpe la disponibilidad de los sistemas. • **Acceso no autorizado**: Hackers que acceden a servidores o estaciones de trabajo para robar o manipular datos.

portátiles que utiliza el personal asistencial y administrativo. • **Dispositivos de red**: Routers, switches, firewalls, que aseguran la conectividad y seguridad en la red interna del hospital.	• **Robo físico de dispositivos**: Sustracción de equipos físicos que contienen datos sensibles. • **Malware y ransomware**: Instalación de software malicioso que compromete la seguridad y la funcionalidad de los dispositivos.
• **Dispositivos de almacenamiento**: Discos duros internos y externos. • **Almacenamiento en la nube**: Plataformas en la nube utilizadas para guardar datos y hacer backups remotos de la información de la entidad (Drive del correo electrónico institucional). • **Dispositivos de backup**: Unidades de almacenamiento NAS (Network Attached Storage) que guardan copias de seguridad de datos críticos de las estaciones de trabajo principales y bases de datos de los servidores. La entidad cuenta con 2 de estos dispositivos.	• **Pérdida de datos**: Daño físico o cibernético a los dispositivos de almacenamiento que puede resultar en la pérdida de datos críticos. • **Acceso no autorizado**: Personas no autorizadas que acceden a los datos almacenados, ya sea en dispositivos locales o en la nube. • **Desastres que destruyen los backups**: Pérdida de copias de seguridad debido a fallos en el hardware o ataques que afectan tanto a los datos originales como a las copias de seguridad.
• Servicio de internet para acceder a plataformas externas.	• **Interrupción del servicio de internet**: Cortes en la conectividad a internet que interrumpen el acceso a servicios y plataformas externas necesarias. • **Ataques de phishing o malware**: Uso de internet para realizar ataques de phishing o introducir malware en la red interna del hospital. • **Acceso no autorizado a plataformas externas**: Hackers que aprovechan vulnerabilidades en las conexiones externas para

	infiltrarse en los sistemas internos del hospital.

IDENTIFICACIÓN DE LAS VULNERABILIDADES

A continuación, se presentan las vulnerabilidades que podrían causar la materialización de las amenazas para cada activo de información:

Activo de información	AMENAZAS	VULNERABILIDADES
• **Registros médicos de pacientes**: Historia clínica, diagnósticos, tratamientos, resultados de laboratorio, imágenes médicas (radiografías, resonancias, etc.). • **Datos administrativos**: Información sobre personal, nóminas, Información sobre ingresos, egresos, presupuestos, y reportes financieros, datos sobre cuentas por cobrar, pagos pendientes, historial de pagos de pacientes y aseguradoras, facturas emitidas a pacientes, aseguradoras o terceros, incluyendo detalles de servicios prestados, costos y pagos recibidos, información sobre acuerdos	• **Acceso no autorizado**: Personal no autorizado podría acceder a registros médicos de pacientes. • **Robo o filtración de datos**: Los registros médicos podrían ser robados o filtrados por un ciberataque, comprometiendo la privacidad de los pacientes. • **Ransomware**: Secuestro de los datos por parte de atacantes, pidiendo un rescate para liberarlos. • **Destrucción de datos**: Pérdida de información médica clave debido a fallos en los sistemas o un ataque malicioso. • **Desastres naturales o fallos de infraestructura**:	• Falta de controles de acceso o permisos mal configurados en los sistemas. • Uso de contraseñas débiles o compartidas entre empleados. • Sistemas sin actualizaciones de seguridad, permitiendo ataques como ransomware. • No contar con copias de seguridad actualizadas o almacenarlas en el mismo entorno que los datos originales.

contractuales relacionados con seguros médicos, servicios externos, y acuerdos comerciales. • **Documentos legales y contratos**: Contratos con proveedores, acuerdos de confidencialidad, licencias de software. • **Planes de continuidad del negocio**: Procedimientos de recuperación ante desastres, planes de contingencia. • **Políticas y procedimientos internos**: Manuales de usuario, procedimientos operativos, políticas.	Desastres físicos como incendios o inundaciones que dañan las instalaciones o sistemas.	
• **Sistema de Gestión Hospitalaria**: Software de administración que maneja citas, registros médicos, inventarios, facturación, información financiera, etc (Dinámica Gerencial). • **Sistema de Información Radiológica (PACS)**: Para el manejo de imágenes médicas y la integración con otros	• **Fallos en el sistema**: Caídas del sistema que pueden interrumpir las operaciones hospitalarias (citas, registros médicos, suministros, etc.). • **Ransomware**: Secuestro del sistema que afecta la disponibilidad de servicios clave (facturación, gestión de pacientes).	• Falta de actualizaciones y parches de seguridad en los sistemas. • Exceso de permisos a usuarios que no necesitan acceso a ciertos módulos. • Configuración deficiente de antivirus. • Falta de monitoreo o

sistemas de diagnóstico. • **Software de mantenimiento**: Herramientas que ayudan a mantener el funcionamiento óptimo de los equipos informáticos, biomédicos e industriales, gestionando las reparaciones, mantenimiento preventivo, historial de mantenimiento y calibración de los dispositivos.	• **Acceso no autorizado**: Acceso no autorizado por parte de personal malintencionado o cibercriminales. • **Integridad de los datos**: Manipulación o alteración de datos relacionados con los pacientes o la facturación. • **Robo de imágenes médicas**: Filtración de imágenes sensibles de los pacientes (radiografías, resonancias). • **Interrupción del servicio**: Caídas del sistema que dificultan la consulta o diagnóstico a tiempo de las imágenes médicas.	auditoría de accesos y modificaciones en los sistemas. • No contar con mecanismos de respaldo adecuados en caso de caídas del sistema.
• **Servidores**: Servidores que alojan bases de datos críticas (por ejemplo, servidor del software Dinámica Gerencial). • **Estaciones de trabajo**: Computadoras de escritorio o portátiles que utiliza el personal asistencial y administrativo.	• **Ataques DDoS**: Sobrecarga de servidores o redes que interrumpe la disponibilidad de los sistemas. • **Acceso no autorizado**: Hackers que acceden a servidores o estaciones de trabajo para robar o manipular datos.	• Uso de software desactualizado o sin soporte. • Exposición a internet sin protecciones adecuadas (firewalls). • Acceso físico sin restricciones o sin monitoreo.

• **Dispositivos de red**: Routers, switches, firewalls, que aseguran la conectividad y seguridad en la red interna del hospital.	• **Robo físico de dispositivos**: Sustracción de equipos físicos que contienen datos sensibles. • **Malware y ransomware**: Instalación de software malicioso que compromete la seguridad y la funcionalidad de los dispositivos.	
• **Dispositivos de almacenamiento**: Discos duros internos y externos. • **Almacenamiento en la nube**: Plataformas en la nube utilizadas para guardar datos y hacer backups remotos de la información de la entidad (Drive del correo electrónico institucional). • **Dispositivos de backup**: Unidades de almacenamiento NAS (Network Attached Storage) que guardan copias de seguridad de datos críticos de las estaciones de trabajo principales y bases de datos de los servidores. La entidad	• **Pérdida de datos**: Daño físico o cibernético a los dispositivos de almacenamiento que puede resultar en la pérdida de datos críticos. • **Acceso no autorizado**: Personas no autorizadas que acceden a los datos almacenados, ya sea en dispositivos locales o en la nube. • **Desastres que destruyen los backups**: Pérdida de copias de seguridad debido a fallos en el hardware o ataques que afectan tanto a los datos originales	• Uso de servicios en la nube sin configuraciones de seguridad adecuadas. • No proteger físicamente los dispositivos de almacenamiento externos (ej. discos duros).

cuenta con 2 de estos dispositivos.	como a las copias de seguridad.	
• Servicio de internet para acceder a plataformas externas.	• **Interrupción del servicio de internet**: Cortes en la conectividad a internet que interrumpen el acceso a servicios y plataformas externas necesarias. • **Ataques de phishing o malware**: Uso de internet para realizar ataques de phishing o introducir malware en la red interna del hospital. • **Acceso no autorizado a plataformas externas**: Hackers que aprovechan vulnerabilidades en las conexiones externas para infiltrarse en los sistemas internos del hospital.	• Empleados accediendo a sitios web y servicios no autorizados desde la red interna. • Falta de monitoreo de tráfico para detectar conexiones sospechosas. • Daños en la infraestructura del proveedor.

6. ANÁLISIS DEL RIESGO INHERENTE

Para cuantificar y clasificar el riesgo inherente, se toma como base la tabla de probabilidad, la tabla de impacto y la matriz de calificación.

Tabla de Probabilidad: La probabilidad es la medida para estimar la ocurrencia del riesgo y se mide con criterios de frecuencia

RARO	El evento puede ocurrir solo encircunstancias excepcionales	No se ha presentado en los últimos 5 años.
IMPROBABLE	El evento puede ocurrir en algúnmomento.	Al menos de 1 vez en los últimos 5 años.
POSIBLE	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 últimoaño.
CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Figura 2. Tabla de Probabilidad

Tabla de Impacto: Son las consecuencias potenciales que genera el hecho que se materialice en el riesgo.

TABLA DE IMPACTO			
TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN**
CONFIDENCIALIDAD EN LA INFORMACIÓN	**1**	**INSIGNIFICANTE**	Se afecta a una persona en particular.
	2	**MENOR**	Se afecta a un grupo de trabajo interno del proceso.
	3	**MODERADO**	Se afecta a todo el proceso.
	4	**MAYOR**	La afectación se da a nivel estratégico.
	5	**CATASTRÓFICO**	La afectación se da a nivel institucional.

CREDIBILIDAD O IMAGEN	**1**	**INSIGNIFICANTE**	Se afecta al grupo de funcionarios y contratistas del proceso
	2	**MENOR**	Se afecta a todos los funcionarios y contratistas de la entidad
	3	**MODERADO**	Se afecta a los usuarios de la Sede Central de la entidad
	4	**MAYOR**	Se afecta a los usuarios de las Direcciones Territoriales.
	5	**CAT AST RÓFICO**	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales
LEGAL	**1**	**INSIGNIFICANTE**	Se producen multas para la entidad.
	2	**MENOR**	Se producen demandas para la entidad.
	3	**MODERADO**	Se producen investigaciones disciplinarias
	4	**MAYOR**	Se producen investigaciones fiscales.
	5	**CATASTRÓFICO**	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control
	1	**INSIGNIFICANTE**	Se tendrían que realizar ajustes a una actividad concreta del proceso.

OPERATIVO	**2**	**MENOR**	Se tendrían que realizar ajustes en los procedimientos del proceso
	3	**MODERADO**	Se tendrían que realizar ajustes en la interacción de procesos.
	4	**MAYOR**	Se presentarían intermitencias o dificultades en la operación del proceso
	5	**CATASTRÓFICO**	Se presentaría paro o no operación del proceso.

Matriz De Calificación, Evaluación Y Respuesta A Los Riesgos: Representa la Zona en la que se encuentra el riesgo a la que se enfrenta inicialmente un proceso o la Entidad en ausencia de controles.

CONCEPTO		IMPACTO				
		1	2	3	4	5
PROBABILIDAD		**INSIGNIFICANTE (1)**	**MENOR (2)**	**MODERADO (3)**	**MAYOR (4)**	**CATASTRÓFICO (5)**
	VALOR	**1**	**2**	**3**	**4**	**5**
RARA VEZ (1)	**1**	**11**	**12**	**13**	**14**	**15**
IMPROBABLE (2)	**2**	**21**	**22**	**23**	**24**	**25**
POSIBLE (3)	**3**	**31**	**32**	**33**	**34**	**35**
PROBABLE (4)	**4**	**41**	**42**	**43**	**44**	**45**
CASI SEGURO (5)	**5**	**51**	**52**	**53**	**54**	**55**

ZONA DE RIESGO BAJA
ZONA DE RIESGO MODERADA
ZONA DE RIESGO ALTA
ZONA DE RIESGO EXTREMA

Basados en las figuras presentadas anteriormente, se presenta el análisis del riesgo inherente para E.S.E Hospital San José del Guaviare:

Activo de información	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
• **Registros médicos de pacientes**: Historia clínica, diagnósticos, tratamientos, resultados de laboratorio, imágenes médicas (radiografías, resonancias, etc.). • **Datos administrativos**: Información sobre personal, nóminas, Información sobre ingresos, egresos, presupuestos, y reportes financieros, datos sobre cuentas por cobrar, pagos pendientes, historial de pagos de pacientes y aseguradoras, facturas emitidas a pacientes, aseguradoras o terceros, incluyendo	**POSIBLE**	**MAYOR**	**ZONA DE RIESGO EXTREMA**

detalles de servicios prestados, costos y pagos recibidos, información sobre acuerdos contractuales relacionados con seguros médicos, servicios externos, y acuerdos comerciales. • **Documentos legales y contratos**: Contratos con proveedores, acuerdos de confidencialidad, licencias de software. • **Planes de continuidad del negocio**: Procedimientos de recuperación ante desastres, planes de contingencia. • **Políticas y procedimientos internos**: Manuales de usuario, procedimientos operativos, políticas.			
• **Sistema de Gestión Hospitalaria**: Software de administración que maneja citas, registros médicos, inventarios, facturación, información	**PROBABLE**	**MAYOR**	**ZONA DE RIESGO EXTREMA**

financiera, etc (Dinámica Gerencial). • **Sistema de Información Radiológica (PACS)**: Para el manejo de imágenes médicas y la integración con otros sistemas de diagnóstico. • **Software de mantenimiento**: Herramientas que ayudan a mantener el funcionamiento óptimo de los equipos informáticos, biomédicos e industriales, gestionando las reparaciones, mantenimiento preventivo, historial de mantenimiento y calibración de los dispositivos.			
• **Servidores**: Servidores que alojan bases de datos críticas (por ejemplo, servidor del software Dinámica Gerencial). • **Estaciones de trabajo**: Computadoras de escritorio o portátiles que utiliza el personal asistencial y administrativo.	**IMPROBABLE**	**MAYOR**	**ZONA DE RIESGO EXTREMA**

• **Dispositivos de red**: Routers, switches, firewalls, que aseguran la conectividad y seguridad en la red interna del hospital.			
• **Dispositivos de almacenamiento**: Discos duros internos y externos. • **Almacenamiento en la nube**: Plataformas en la nube utilizadas para guardar datos y hacer backups remotos de la información de la entidad (Drive del correo electrónico institucional). • **Dispositivos de backup**: Unidades de almacenamiento NAS (Network Attached Storage) que guardan copias de seguridad de datos críticos de las estaciones de trabajo principales y bases de datos de los servidores. La entidad cuenta con 2 de estos dispositivos.	**POSIBLE**	**MAYOR**	**ZONA DE RIESGO EXTREMA**
• Servicio de internet para acceder a plataformas externas.	**PROBABLE**	**MAYOR**	**ZONA DE RIESGO EXTREMA**

7. IDENTIFICACIÓN DE CONTROLES Y PLAN DE TRATAMIENTO DE RIESGOS

Activo de información	Opciones de manejo del riesgo	Descripción del control	Responsable	Periodo
• **Registros médicos de pacientes**: Historia clínica, diagnósticos, tratamientos, resultados de laboratorio, imágenes médicas (radiografías, resonancias, etc.). • **Datos administrativos**: Información sobre personal, nóminas, Información sobre ingresos, egresos, presupuestos, y reportes financieros, datos sobre cuentas por cobrar, pagos pendientes, historial de pagos de pacientes y	Reducir el riesgo	• Realizar copias de seguridad automáticas con almacenamiento en ubicaciones seguras y fuera del entorno productivo. • Entrenar al equipo en buenas prácticas de seguridad de la información.	Oficina de sistemas	Trimestral

aseguradoras, facturas emitidas a pacientes, aseguradoras o terceros, incluyendo detalles de servicios prestados, costos y pagos recibidos, información sobre acuerdos contractuales relacionados con seguros médicos, servicios externos, y acuerdos comerciales. • **Documentos legales y contratos**: Contratos con proveedores, acuerdos de confidencialidad, licencias de software. • **Planes de continuidad del negocio**: Procedimientos de recuperación ante desastres, planes de contingencia.				

• **Políticas y procedimientos internos**: Manuales de usuario, procedimientos operativos, políticas.				
• **Sistema de Gestión Hospitalaria**: Software de administración que maneja citas, registros médicos, inventarios, facturación, información financiera, etc (Dinámica Gerencial). • **Sistema de Información Radiológica (PACS)**: Para el manejo de imágenes médicas y la integración con otros sistemas de diagnóstico. • **Software de mantenimiento** : Herramientas que ayudan a mantener el funcionamiento óptimo de los		• Mantener el software actualizado con las últimas versiones y aplicar parches de seguridad. • Configurar tiempos de expiración de sesión y bloqueos tras intentos fallidos. • Generar copias de seguridad automáticas y realizar pruebas de recuperación. • Revisar y validar los permisos de usuarios periódicamente.	• Oficina de sistemas	Trimestral

equipos informáticos, biomédicos e industriales, gestionando las reparaciones, mantenimiento preventivo, historial de mantenimiento y calibración de los dispositivos.				
• **Servidores**: Servidores que alojan bases de datos críticas (por ejemplo, servidor del software Dinámica Gerencial). • **Estaciones de trabajo**: Computadoras de escritorio o portátiles que utiliza el personal asistencial y administrativo. • **Dispositivos de red**: Routers, switches, firewalls, que aseguran la conectividad y seguridad en la red interna del hospital.	Reducir el riesgo	• Aplicar configuraciones seguras, deshabilitar servicios innecesarios y usar firewalls. • Tener backups en diferentes ubicaciones y servidores redundantes. • Configurar reglas estrictas de acceso y bloquear conexiones sospechosas.	• Oficina de sistemas	Trimestral

• **Dispositivos de almacenamiento**: Discos duros internos y externos. • **Almacenamiento en la nube**: Plataformas en la nube utilizadas para guardar datos y hacer backups remotos de la información de la entidad (Drive del correo electrónico institucional). • **Dispositivos de backup**: Unidades de almacenamiento NAS (Network Attached Storage) que guardan copias de seguridad de datos críticos de las estaciones de trabajo principales y bases de datos de los servidores. La entidad cuenta con 2 de estos dispositivos.	Reducir el riesgo	• Gestionar permisos de acceso en la nube y en servidores locales. • Bloquear el uso de USB no autorizados mediante políticas de grupo (GPO).	• Oficina de sistemas	Trimestral

• Servicio de internet para acceder a plataformas externas.	Reducir el riesgo	• Bloquear sitios web no autorizados. • Configurar firewalls. • Backup del servicio de internet.	• Oficina de sistemas	Trimestral

8. BIBLIOGRAFÍA

Guía 7 Gestión de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea. Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Función pública, octubre 2018, versión 4. Anexo 4, lineamiento para la gestión de riesgos de seguridad digital en entidades públicas. Ministerio de tecnologías de la información y las comunicaciones, 2018.