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

HOSPITAL DEPARTAMENTAL SAN ANTONIO PITALITO HUILA
2023

CONTROL DE DOCUMENTO Y DISTRIBUCIÓN:

Control del Documento

	Nombre	Cargo	Dependencia	Fecha
Autor	Gerardo Gómez Cortes Edna Rocio Plazas Garcia	Asesor Sistemas de Información Especialista seguridad de la Información	Sistemas de Información Mesa de ayuda Indigo Technologies SAS	20 de enero de 2023
Revisión	Ana Luz Trujillo Muñoz	Subgerente Administrativa y Financiera	Subgerencia Administrativa y Financiera	27 de enero de 2023
Aprobación	Comité de Gestión y Desempeño			
	Acta No. 001 del 27 de enero de 2023			
	Presidente Comité	Diana Victoria Muñoz Muñoz - Gerente		
Adopción	Resolución Gerencial No. 037		Fecha: 27 de enero de 2023	

Control de los Cambios

Versión No.	Fecha de Aprobación	Descripción de los Cambios	Solicitó
1.0	Resolución No. 213 del 16/09/2021	Levantamiento del procedimiento	
2.0	Resolución No. 053 del 29/01/2021	Actualización del documento	
3.0	Resolución No. 027 del 27/01/2022	Actualización del documento	
4.0	Resolución No. 037 del 27/01/2023	Actualización del documento	

1. OBJETIVO

Presentar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información SGSI de la E.S.E Hospital Departamental San Antonio de Pitalito, de tal forma que se definen y aplican los controles con los cuales se busca mitigar la materialización de los riesgos de seguridad de la información en la entidad. De esta forma, se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información dentro de la institución, se mantenga la integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

El Plan de tratamiento de riesgos de seguridad de la información es aplicable a todos los procesos de la E.S.E Hospital Departamental San Antonio de Pitalito, con alcance a los colaboradores de todos los niveles.
Este plan está orientado a gestionar los riesgos de seguridad digital asociados a las plataformas tecnológicas y servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades asociadas al modelo de operación por procesos adoptados en la entidad.

3. TERMINOS Y DEFINICIONES

Para facilitar la comprensión del presente documento, se definen los siguientes términos:

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Aceptación del riesgo:** Decisión informada de tomar un riesgo particular.
- **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- **Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización.
- **Asumir/Aceptar:** La entidad acepta el riesgo en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección y lo asume conociendo los efectos de su posible materialización.
- **Causa:** Origen, comienzo de una situación determinada que genera un efecto o consecuencia.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Resultado de un evento que afecta los objetivos.
- **Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control:** Medida que modifica el riesgo.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO31000:2013.
- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- **HDSAP:** Hospital Departamental San Antonio de Pitalito.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y

amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- **Información:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **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.
- **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- **MSPI:** Modelo de Seguridad y privacidad.
- **Política de seguridad de información:** Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.
- **Probabilidad:** Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
- **Riesgos de seguridad digital:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **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 Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información:** Parte del sistema de gestión general del Instituto, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo" (Icontec Internacional, 2011).
- **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información.

4. MARCO LEGAL Y/O CONCEPTUAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Resolución 500 de marzo 10 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.
- Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).
- Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".

- Ley 1712 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”.
- Decisión Andina 351 de 2015 “Régimen común sobre derecho de autor y derechos conexos”.
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.
- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.
- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2018.
- Norma Técnica Colombiana ISO27001:2013.
- Norma Técnica Colombiana ISO31000:2013.

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

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información – SGSI del Hospital Departamental San Antonio de Pitalito, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información. De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo u oportunidad.

El Plan de Contingencia informático es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones – TIC’S del HSANPITALITO, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Acciones para considerar:
• Antes, como un plan de respaldo o de prevención para mitigar los incidentes.
• Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
• Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término “incidente” en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en el HSANPITALITO.

6. PUNTOS DE CONTROL

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos del Hospital Departamental San Antonio de Pitalito, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

6.1 MATRIZ DE RIESGOS INSTITUCIONAL

La entidad ha establecido un procedimiento para la gestión integral del riesgo y como producto de su aplicación ha elaborado la matriz de riesgos institucional, la cual se encuentra identificada dentro del SGSI (Sistema de gestión de seguridad de la Información). La matriz muestra el consolidado de los riesgos del proceso de Gestión de Información, clasificados de la siguiente manera:

Tabla 1. Riesgos de proceso

RIESGOS DE PROCESO
Subregistros asistenciales y administrativos
No disponibilidad de Servicios TI
Perdida de la información
Usuarios insatisfechos con el servicio de soporte técnico de la mesa de ayuda
Software desarrollado desalineado con el proceso
No disponibilidad de capital para invertir en recursos de TI
Uso de software ilegal
Falla tecnológica y de redes
Inapropiado almacenamiento y custodia de historias clínicas y documentación

Tabla 2.Riesgos de sistemas de información

RIESGOS DE SISTEMAS DE INFORMACIÓN
Daño por calentamiento en el cuarto del servidor principal
Colapso estructural por movimiento sísmico que pueda causar daño en los servidores
Espionaje remoto de bases de datos de historias clínicas y financiera
Pérdida de información vital para la operación del negocio

Incumplimiento en la disponibilidad del personal de soporte

Para efectos del presente Plan de Tratamiento de Riesgos, tomamos los riesgos de sistemas de información y haciendo énfasis en los riesgos que en el mapa de calor se encuentren en naranja y rojo, producto de este estudio da como resultado la siguiente matriz de riesgos.

RIESGO	CAUSAS	CONSECUENCIAS	CONTROLES ACTUALES	P	I	NR	NUEVOS CONTROLES PROPUESTOS	RESPONSABLE	PLAZO	INDICADOR	SEGUIMIENTO
Falla en la seguridad e integralidad de la información	1.Insuficiencia de infraestructura tecnológica que garantice custodia, accesibilidad e integralidad de dato. 2.Falta de priorización la compra de herramientas informáticas. 3. Ataques informáticos.	Fallas en la oportunidad de la atención que puede generar insatisfacción, deserción del paciente e implicaciones legales Insatisfacción del cliente interno y externo	El proceso de Gestión de la Información cuenta con los siguientes mecanismos que permitirá mitigar el riesgo así: - Plan anual de adquisiciones - HSP-SI-P19 Instructivo Mesa de Servicio. - Manual de Seguridad de la Información. - Procedimiento de Uso y apropiación	3	5	RIESGO ALTO	1. Monitoreo y configuración de Firewall perimetral SONICWALL. 2. Utilización de herramientas para protección de correos institucionales. 3. Aplicar todas las políticas de seguridad de la información aprobadas. 4. Despliegue y educación en seguridad de la información.	proceso de Gestión de la Información	2023	**Indicador 1.** Porcentaje de ataques informáticos Controlados al sistema de información: número de ataques controlados en el periodo/ Total de ataques informáticos en el periodo*100. **Indicador 2.** % Inspecciones Realizadas de seguridad de la información: Cantidad de inspecciones de seguridad realizadas / total de inspecciones programadas*100 (Meta: 100%). **Indicador 3.** % Capacitaciones realizadas en el periodo: Numero de capacitaciones ejecutadas/Total de capacitaciones programadas*100. (Meta: 100%)	proceso de Gestión de la Información
Manejo inadecuado de la protección de datos personales que afectan la confidenciali	1. El personal involucrado en la recopilación e ingreso de datos clínicos no salvaguarda la confidencialidad del dato. 2. La información que se filtra	Violación a la privacidad del usuario y su familia e implicaciones legales.	El proceso de Gestión de la Información cuenta con los siguientes mecanismos que permitirá mitigar el riesgo así: • HSP SI POL 23 POLÍTICA DE CONFIDENCIALIDAD,	1	3	RIESGO MEDIO	1. Actualizaciones continuas del sistema de información. 2. Planes de contingencia para prevenir eventos adversos	proceso de Gestión de la Información	2023	**Indicador 2.** % Inspecciones Realizadas de seguridad de la información: Cantidad de inspecciones de seguridad realizadas / total de inspecciones	proceso de Gestión de la Información

dad de la información	confidencial de los pacientes puede afectar su entorno social.		PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES. • HSP GI F- 01 ACUERDO DE CONFIDENCIALIDAD PERSONAL DE PLANTA. • HSP GI F- 02 ACUERDO DE CONFIDENCIALIDAD- CONTRATISTA Y/O AFILIADOS PARTICIPES INSTRUCTIVO DE USO Y PERMISOS DE NAVEGACIÓN. • HSP GI P 03 PROCEDIMIENTO: SOLICITUD COPIA DE HISTORIAS CLÍNICAS. • HSP SI P 06 PROCEDIMIENTO DE CONTROL DE ACCESOS LÓGICOS HSP-SI-POL-26 INSTRUCTIVO DE USO Y PERMISOS DE NAVEGACIÓN				relacionados con la información.			programadas*100 (Meta: 100%).	
Falta de Calidad en la captura de datos de los registros clínicos y administrativos	1. Dificultad en la programación de auditorías que se deben realizar en las Historias clínicas para asegurar calidad del dato. 2. Constante cambio de normatividad que generan	Toma de decisiones inadecuadas a nivel directivo	El proceso de Gestión de la Información cuenta con el siguiente mecanismo para asegurar la calidad en la captura del dato. HSP-GI XX PROCEDIMIENTO GESTION DEL DATO.	1	3	RIESGO MEDIO	1. Capacitación a usuarios responsables del registro de información 2. Validación de fuentes de información	proceso de Gestión de la Información	2023	**Indicador:** % Retroalimentación en la calidad del dato. Formula: Número de inconsistencias encontradas y socializadas / Total de inconsistencias encontradas *100.	proceso de Gestión de la Información

	solicitudes de información que no se han capturados.										
Manejo y uso inadecuado de la tecnología no biomédica	1. Falta de planeación para la gestión de la tecnología en términos de actualización, parametrización, capacidad, copias de seguridad y capacitación. 2. Falta de conocimiento de uso de la tecnología y cambio de normatividad del sector salud.	Deficiencia en los procesos misionales y apoyo que generan baja productividad.	El proceso de Gestión de la Información cuenta con el siguiente mecanismo para el hacer seguimiento del uso adecuado de la tecnología no biomédica: HSP-SI-P-08 PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD	1	2	RIESGO BAJO	1. copias de seguridad y equipos de backup. 2.Sencibilización sobre buen manejo de los equipos.	proceso de Gestión de la Información	2023	**Indicador:** % Incidentes del parque computacional (Equipo de cómputo, periférico, Escáner, Impresoras) Número de incidentes del parque computacional presentados en el periodo / Total de equipos del parque computacional) * 100.	proceso de Gestión de la Información

6. ESTRATEGIAS Y/O LINEAS DE ACCION

La ejecución de este plan consiste en llevar a cabo la implementación de los controles propuestos en la matriz anterior, procurando que se realicen dentro de los tiempos establecidos y sean desarrolladas por los responsables asignados.
Para poder llevar a cabo con éxito la ejecución es importante recalcar el compromiso de la Alta dirección para asignar los recursos económicos necesarios a las actividades que así lo requieran.

7. INDICADORES Y METAS

Como se observa en la tabla de la matriz anterior, por cada riesgo y por cada control propuesto se han fijado indicadores individuales, pero a nivel general es pertinente establecer un indicador que agrupe todas las actividades el cual quedaría de la siguiente manera y sirve para medir la eficacia en la ejecución del plan:

INDICADOR	FORMULA	META	RESPONSABLE
Índice de Cumplimiento de Actividades	$\frac{\#\ de\ Actividades\ Cumplidas}{\#\ de\ Actividades\ Programadas} * 100\%$	100%	Mesa de ayuda

8. DOCUMENTOS Y REGISTROS RELACIONADOS

- Política de Confidencialidad, Privacidad y Tratamiento de Datos Personales
- Política General de Seguridad y Privacidad de la Información
- Política Desarrollo Seguro de Software
- Política Claves de Acceso Usuarios
- Política de seguridad física y del entorno
- Política de seguridad para relación con proveedores
- Políticas De Buenas Prácticas En Seguridad De La Información
- Política De Respaldo De Información
- Procedimiento de responsabilidad de la seguridad de la información
- Procedimiento de gestión de activos
- Procedimiento de seguridad ligada a los recursos humanos

- Procedimiento de seguridad en las comunicaciones y operaciones
- Procedimiento de control de acceso lógico
- Procedimiento de adquisición, desarrollo y mantenimiento de sistemas informáticos
- Procedimiento para publicación de información en la página web institucional
- Procedimiento de gestión de incidentes de seguridad
- Procedimiento de gestión de la continuidad del negocio
- Procedimiento de cumplimiento
- Procedimiento de Instalación de software
- Procedimiento de copias de seguridad base de datos
- Procedimiento de copias de seguridad de equipos de cómputo usuarios
- Procedimiento de mantenimiento de equipos de computo
- Procedimiento de restauración de base de datos
- Procedimiento de acceso al data center
- Procedimiento de aceptación de pruebas para actualización o liberación

9. RESPONSABLES

Subgerencia Administrativa y financiera.
Asesor de Sistemas de información.
Administrador mesa de servicio de TI.
Profesional Especializada en Seguridad Informática.
Coordinadores de procesos

10. REFERENCIAS BIBLIOGRAFICAS

- https://sisteseg.com/blog/wp-content/uploads/2018/11/Metodologia-para-Gesti%C3%B3n-de-Riesgos-V-1.0.pdf
- https://1library.co/document/yjmjokky-iso-27005-pdf.html