
	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2			CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN			
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			

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



HOSPITAL DEPARTAMENTAL SAN ANTONIO PITALITO HUILA 2022

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		

CONTROL DE DOCUMENTO Y DISTRIBUCIÓN:


Control del Documento

	Nombre	Cargo	Dependencia	Fecha
Autor	Gerardo Gómez Cortes	Asesor Sistemas de Información	Sistemas de Información	18 de enero de 2022
	Edna Rocio Plazas Garcia	Especialista seguridad de la Información	Mesa de ayuda Indigo Technologies SAS	
Revisión	Ana Luz Trujillo Muñoz	Subgerente Administrativa y Financiera	Subgerencia Administrativa y Financiera	19 de enero de 2022
Aprobación	Comité de Gestión y Desempeño			
	Acta No. 01 del 27 de enero de 2022			
	Presidente Comité	Diana Victoria Muñoz Muñoz - Gerente		
Adopción	Resolución Gerencial No. 027		Fecha: 27 de enero de 2022	

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	

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2			CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN			
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			

1. OBJETIVOS

1.1 Objetivo General

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI del HDSAP; 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 el Hospital Departamental San Antonio de Pitalito. 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 esta y así las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

1.2 Objetivos Específicos


- Identificar y analizar posibles riesgos que pueden afectar las operaciones y procesos informáticos de la institución.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
- Establecer actividades con todos los responsables de los procesos y de la gestión del riesgo de seguridad para la implementación de los planes de tratamiento del riesgo.
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.

2. ALCANCE

Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en el Hospital Departamental San Antonio de Pitalito, la Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

Esto se debe realizar siguiendo los lineamientos nacionales y locales, de igual manera se debe hacer uso de buenas prácticas con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	3

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		


El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que superen el NRA (nivel de riesgo aceptable), de igual manera se deben monitorear los riesgos residuales periódicamente según la planeación de la entidad.

3. TERMINOS Y DEFINICIONES

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


- **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.
- **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.
- **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.
- **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 evalúa.
- **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.

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	4

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		


- 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.
- Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
- MSPi: Modelo de Seguridad y privacidad.

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	5

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		

- 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.
- 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.
- Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.
- 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.


FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	6

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA 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.

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	7

 E.S.E Hospital Departamental San Antonio de Pitalito	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2			CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN			
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN			
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			

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 HSPANPITALITO, 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 HSPANPITALITO.

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.

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	8

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		

5.1 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

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

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 cinco (5) 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.

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	9



E.S.E Hospital Departamental
San Antonio de Pitalito

EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2

PROCESO: GESTIÓN DE LA INFORMACIÓN

SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**CÓDIGO:
HSP-GI-
27/01/2022
Versión:
3.0**



**ESE HOSPITAL DEPARTAMENTAL SAN ANTONIO
PITALITO - HUILA
NIT: 891.180.134 - 2**

**Código de Formato:
versión:
Fecha de Aprobación:**

MATRIZ DE RIESGOS 2022

PROCESO		GESTIÓN DE LA INFORMACIÓN												
OBJETIVO DEL PROCESO		Implementar nuevos modelos de gestión de la tecnología, la información y las comunicaciones con base en herramientas que permitan mejorar los aspectos misionales y estratégicos de la Organización.												
SUBPROCESO SERVICIO	RIESGO	CLASIFICACIÓN	CAUSAS	CONSECUENCIAS	CONTROLES ACTUALES	P	C	NR	NR	NUEVOS CONTROLES PROPUESTOS	RESPONSABLE	PLAZO	INDICADOR	SEGUIMIENTO
Todas las áreas	Falla en la seguridad e integridad de la información	Seguridad de la información	1. Revelar y compartir contraseñas 2. Contraseñas débiles	1. Acceso no autorizado a los sistemas 2. manipulación y adulteración de información 3. Pérdida de información	1. Procedimiento para asignar usuarios y contraseñas 2. Manual de políticas de seguridad de la información	2	5	10	RIESGO ALTO	1. Aplicar todas las políticas de seguridad de la información aprobadas. 2. Despliegue y educación en seguridad de la información.	Líder Gestión de la Información Prof Esp. Gestión de la Información y mesa de ayuda	2022	% Capacitaciones realizadas en el periodo: Numero de capacitaciones ejecutadas/Total de capacitaciones programadas * 100%	Gestión de la información - Oficina Control Interno
Todas las áreas	Mal funcionamiento del sistema de información INDIGO	Seguridad de la información	1. Deficiencia en procedimientos de seguridad de la información 2. Deficiente	1. Afecta negativamente en la prestación del servicio. 2. Información inoportuna a clientes internos y externos.	1. Mesa de ayuda 2. Análisis de causas de las dificultades presentadas frente a lo esperado.	4	3	12	RIESGO ALTO	1. Actualizaciones continuas del sistema de información. 2. Planes de contingencia para prevenir eventos	Líder Gestión de la Información Prof Esp. Gestión de la Información	2022	Número de horas de disponibilidad del sistema de información en el periodo/	Gestión de la información - Oficina Control Interno

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	1



E.S.E Hospital Departamental
San Antonio de Pitalito

EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2

PROCESO: GESTIÓN DE LA INFORMACIÓN


SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**CÓDIGO:
HSP-GI-
27/01/2022
Versión:
3.0**

			cobertura a red de internet en áreas en donde se requiere para cumplir con la misión operativa de la organización						adversos relacionados con la información.	n y mesa de ayuda		Total horas del periodo*100 %		
			3. Deficiente capacidad de número de equipos para el procesamiento de la información.						3. Estudios y verificación en que áreas se requiere ampliación de acceso a redes de internet					
			4. Error en las actualizaciones											
Todas las áreas	Virus y malware informático	Seguridad de la información	1. Antivirus Caducado 2. Falta de mantenimiento. 3. Desconocimiento del manejo adecuado de los equipos e internet.	1. Fallas en el funcionamiento de los equipos de cómputo de los usuarios cuando sea el caso. 2. Pérdida de documentos o información importante alojada en los servidores. 3. Secuestro de datos.	1. Servicio de soporte técnico 24/7 2. Rondas de mantenimiento preventivo de equipos por año	2	3	6	RIESGO MEDIO	1. Realizar capacitaciones periódicas para el buen uso de los equipos. 2. Mantenimiento periódico de los equipos.	Líder Gestión de la Información Prof Esp. Gestión de la Información y mesa de ayuda	2022	% Inspecciones Realizadas de seguridad de la información: Cantidad de inspecciones de seguridad realizadas / total de inspecciones	Gestión de la información - Oficina Control Interno

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD 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	$\frac{\# \text{ de Actividades Cumplidas}}{\# \text{ de Actividades Programadas}} * 100\%$	100%	Mesa de ayuda

8. DOCUMENTOS Y REGISTROS RELACIONADOS

- Política de Seguridad de la 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 Física en las Instalaciones
- Procedimiento de Seguridad en las Comunicaciones y Operaciones
- Procedimiento de Control de Acceso Lógico
- Procedimiento de Adquisición, Desarrollo y Mantenimiento de Sistemas Informáticos

9. RESPONSABLES

FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2		CÓDIGO: HSP-GI- 27/01/2022 Versión: 3.0
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN		
	NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		

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

10. REFERENCIAS BIBLIOGRAFICAS

- <https://sisteseq.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>



FECHA:	Elaboración: 06/09/2021	Aprobación	Adopción	Versión:	Hoja:
	Modificación: 27/01/2022	Acta No. 001 del 27/01/2022 Comité Institucional de Gestión y desempeño	Resolución No. 027 del 27/01/2022	3.0	2