EMPRESA SOCIAL DEL ESTADO

PASTO SALUD E.S.E

NIT.900091143-9

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

VERSIÓN 10.0

SAN JUAN DE PASTO
2025

TABLA DE CONTENIDO

CONTROL DE CAMBIOS

E: Elaboración del documento
M: Modificación del documento
X: Eliminación del documento

Versión	CONTROL DE CAMBIOS	INFORMACION DE CAMBIOS					Acto Administrativo de Adopción
		E	M	X	Actividades o Justificación del cambio	Elaboró / Actualizó	
10.0	Actualización Documento Plan de tratamiento de riesgos de seguridad y privacidad de la información		X		**Justificación:** Se actualizaron los siguientes capítulos: Introducción, Objetivos, Alcance, Política, Marco legal, Matriz de Riesgos y Plan de acción 2025	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Profesional Universitario	Resolución No 089 del 27 de enero 2025
9.0	Actualización Documento Plan de tratamiento de riesgos de seguridad y privacidad de la información		X		**Justificación:** Se actualiza la Matriz de riesgos vigencia 2024 Se actualizan las Actividades para vigencia poa 2024	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Profesional Universitario	Resolución No 0080 del 26 de enero 2024
8.0	Elaboración del Documento Plan de tratamiento de riesgos		X		**Justificación:** Se realiza ajuste a los objetivos específicos, Modelo de operación del Sistema de Gestión de la Seguridad, Actividades y cronograma Vigencia 2021	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 058-28-01-2021
7.0	Elaboración del Documento Plan de tratamiento de riesgos	X			**Justificación** La alta gerencia de la Empresa Social del Estado Pasto Salud, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno digital. , elabora el Modelo de Seguridad y Privacidad de la Información. Solicitudes del decreto 612 de 2018 y Decreto 1078 de 2015.	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 093-29-01-2020

RESOLUCIÓN No. 089
(27 de enero del 2025)

"Por la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2025"

EL GERENTE

En uso de sus atribuciones legales y en especial a la conferidas por el Acuerdo No. 004 del 2006 emanado del Concejo Municipal de Pasto, Ley 1753 de 2015 y Decreto 1083 del 2015 y,

CONSIDERANDO:

Que mediante el Decreto 612 del 4 de abril del 2018, se fijan directrices para la integración de los planes institucionales y estratégicos del Plan de Acción por parte de las entidades del Estado, en su artículo 1, adiciona entre otros el artículo 2.2.22.3.14 al capítulo 3 del Título 22 del parte 2 del Decreto 1083 del 2015. Único Reglamentario del Sector de Función Pública, la cual dispone que las entidades de Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, deberán integrar los planes institucionales y estratégicos, entre ellos el Plan Anual

Que el artículo 2 del Decreto Presidencial 612 del 4 de abril de 2018 señala que las entidades del Estado de manera progresiva deberán integrar los planes institucionales y estratégicos y publícalos en la página web de la entidad.

Que mediante el Decreto 1008 de 14 de junio de 2018 se establece que la seguridad y privacidad de la información, es uno de los habilitadores transversales de la nueva Política de Gobierno Digital.

Que mediante Acta No 001-2025 del Comité Institucional de Gestión y Desempeño del día 27 de enero de 2025 se presentó, se revisó y se aprobó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2025, el cual se pretende adoptar mediante el presente acto administrativo.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO. - Adoptar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2025", documento que hace parte integral de la presente resolución.

ARTÍCULO SEGUNDO. - El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo principal gestionarlos riesgos de seguridad y privacidad de la información, a través de la metodología establecida, facilitando la identificación del riesgo, las oportunidades, el análisis, la valoración e implementación de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E	RESOLUCIONES			
	VERSIÓN	PROCESO/SERVICIO	CODIGO	NUM
	6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-R	092
	OFICINA DE COMUNICACIONES Y SISTEMAS			

ARTÍCULO TERCERO. - Publíquese el presente acto administrativo en la página web de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2025".

ARTÍCULO CUARTO. - La presente resolución rige a partir de la fecha de su expedición y deroga las disposiciones contrarias a este.

PUBLÍQUESE Y CÚMPLASE

DIEGO FERENANDO MORALES ORTEGÓN
Gerente

Proyectó: William Ricardo Montenegro Guevara / Profesional Universitario

INTRODUCCIÓN

En la actualidad, las empresas reconocen que la información es su principal activo, lo que resalta la importancia de identificarla y protegerla adecuadamente. Este desafío se centra en garantizar un tratamiento, manejo y clasificación de la información bajo una administración y custodia efectiva.

La seguridad de la información tiene como objetivo principal proteger los activos informativos en cualquiera de sus estados, enfrentando amenazas y brechas que puedan comprometer los principios fundamentales de confidencialidad, integridad y disponibilidad.

El plan de tratamiento de riesgos busca prevenir incidentes mediante la planificación e implementación de acciones y medidas de control de seguridad. Estas acciones permiten gestionar y reducir los riesgos e impactos asociados, minimizando la afectación a la entidad en caso de que se materialicen.

1 OBJETIVO GENERAL

Reducir y controlar los riesgos asociados a la seguridad y privacidad de la información, minimizando la probabilidad e impacto de incidentes, y garantizando la protección de los activos de información de la Empresa Social del Estado Pasto Salud.

1.1. OBJETIVOS ESPECÍFICOS

- Identificar, analizar y evaluar los riesgos relacionados con la seguridad y privacidad de la información, considerando vulnerabilidades y amenazas específicas.

- Implementar y gestionar acciones correctivas y preventivas frente a incidentes de seguridad y privacidad, asegurando una respuesta efectiva y oportuna.

2 ALCANCE

El plan de riesgos aplica a todos los procesos, activos y sistemas de información de la Empresa Social del Estado Pasto Salud E.S.E., priorizando la identificación, gestión y mitigación de riesgos clasificados como altos y extremos, con el fin de garantizar la seguridad, privacidad y continuidad de la información.

3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En Pasto Salud E.S.E. nos comprometemos a mantener la confidencialidad, integridad y disponibilidad de la información mediante la implementación de un Modelo de Seguridad y Privacidad, gestionando integralmente los riesgos y cumpliendo los requisitos legales que aseguran la privacidad de la información de nuestros grupos de interés, con un enfoque en la mejora continua.

4 MARCO LEGAL

El presente plan de riesgos se fundamenta en un conjunto de normas y estándares nacionales e internacionales que garantizan la seguridad, privacidad y adecuada gestión de la información. Estas disposiciones son esenciales para el cumplimiento normativo y la implementación de buenas prácticas en la Empresa Social del Estado Pasto Salud E.S.E.

Normativa Nacional

Ley 1273 de 2009
- Modifica el Código Penal para introducir el bien jurídico tutelado denominado "Protección de la Información y de los Datos".
- Establece medidas para preservar la integridad de los sistemas que utilicen tecnologías de la información y las comunicaciones (TIC).
- Penaliza conductas como el acceso abusivo, la interceptación de datos informáticos, el daño a sistemas informáticos y la utilización indebida de software malicioso.

Ley 1581 de 2012 (Ley de Protección de Datos Personales)
- Regula el tratamiento de datos personales para garantizar los derechos de privacidad, libertad y seguridad de la información.
- Exige la implementación de medidas de seguridad para proteger los datos personales contra accesos no autorizados, pérdida, uso indebido o alteración.

Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector Comercio, Industria y Turismo)
- Reglamenta parcialmente la Ley 1581 de 2012, incluyendo disposiciones sobre medidas de seguridad para el tratamiento de datos personales.

Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)
- Regula el acceso a la información pública, estableciendo la obligación de las entidades públicas de garantizar la disponibilidad, integridad y confidencialidad de la información que manejan.

Normativa Internacional

ISO/IEC 27001:2013
- Estándar internacional que proporciona un marco para la gestión de la seguridad de la información.
- Define los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO/IEC 27002:2013
- Proporciona un conjunto de buenas prácticas para la gestión de la seguridad de la información, enfocándose en la selección, implementación y gestión de controles.

- Complementa la ISO/IEC 27001 al ofrecer directrices prácticas para fortalecer la seguridad de la información.

ISO/IEC 31000:2018 (Gestión de Riesgos)
- Establece principios y directrices para la gestión del riesgo en cualquier organización, aplicable al contexto de la seguridad de la información.
- Promueve un enfoque sistemático y estructurado para identificar, evaluar y mitigar riesgos.

ISO/IEC 22301:2019 (Gestión de Continuidad del Negocio)
- Estándar internacional que ayuda a las organizaciones a prepararse para garantizar la continuidad de sus operaciones frente a incidentes que puedan interrumpir los procesos críticos.

5 GLOSARIO

Riesgo: Es toda posibilidad de ocurrencia de una situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

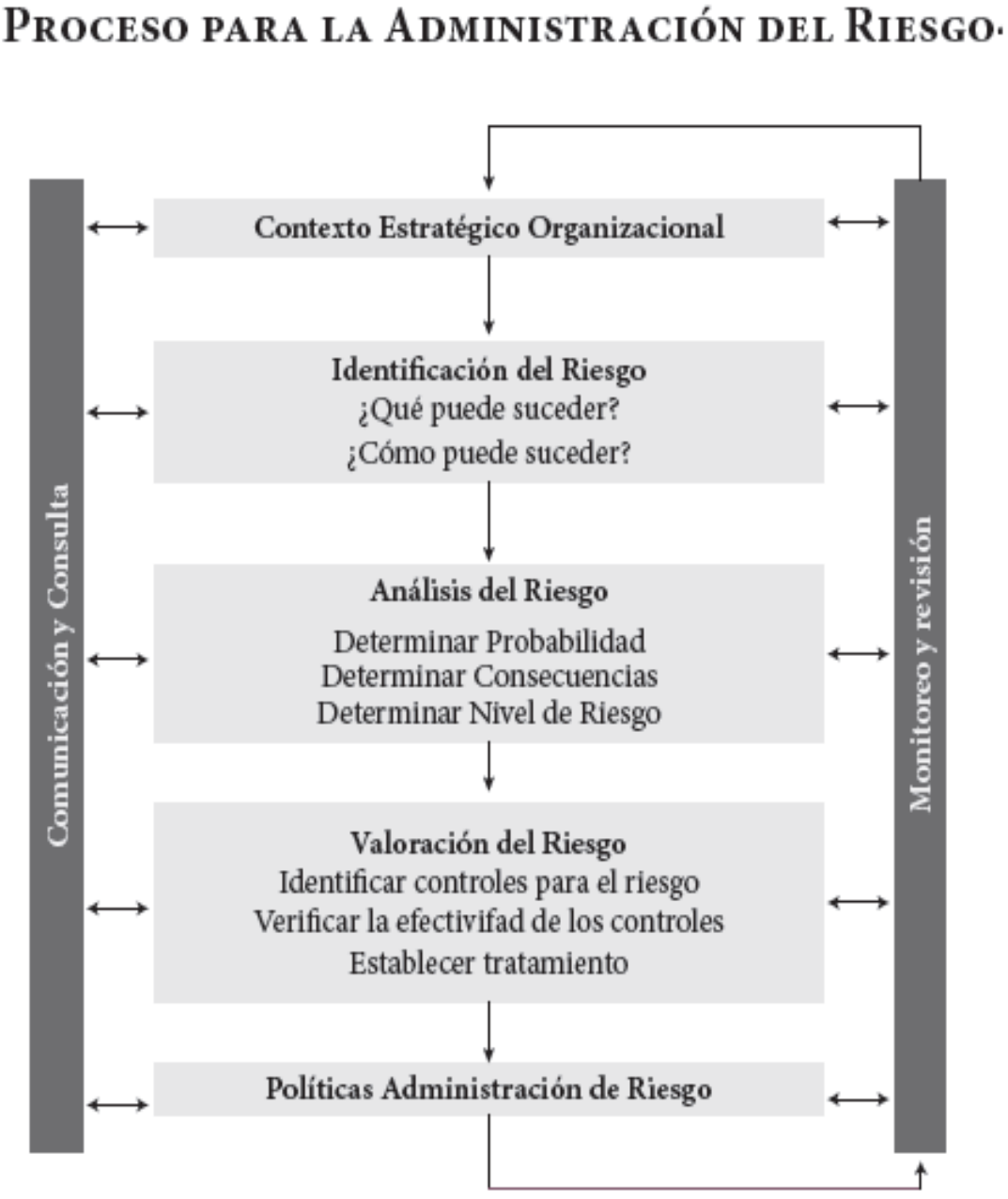
Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Control: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

6 METODOLOGÍA Y OPERACIÓN DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSI



Fuente: Dafp

7 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

7.1 IDENTIFICACIÓN DE AMENAZAS

D: Deliberadas A: Accidentales E: Ambientales

7.1.1 Amenazas Comunes

TIPO	AMENAZA	ORIGEN
Daño Físico	Fuego	A,D,E
	Agua	A,D,E
	Destrucción de equipos	A,D,E
	Deterioro (Polvo)	A,D,E
Eventos Naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Inundación	E
Perdida de los servicios esenciales.	Falla en la fibra óptica y equipos de radio y telecomunicaciones	A,D,A
Seguridad y Privacidad de la información	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D
	Datos provenientes de fuentes no confiables	A,D
	Manipulación con hardware	D
	Manipulación con software	D
Fallas Técnicas	Fallas del equipo	A,D,E
	Mal funcionamiento del equipo	A,D,E
	Saturación del sistema de información	D
	Mal funcionamiento del software	A,D
	Incumplimiento en el mantenimiento del sistema de información y del hardware.	D
Acciones No Autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D

7.1.2 Amenazas Humanas

FUENTE DE AMENAZA	MOTIVACIÓN	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 - Penetración en el sistema - Manipulación en el sistema
Espionaje	Ventaja competitiva Espionaje económico	- 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 y despedidos)	- Curiosidad - Ego - Inteligencia - Ganancia monetaria - Venganza - Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación	- 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 - Sabotaje del sistema - Acceso no autorizado al sistema.

8 IDENTIFICACIÓN DE VULNERABILIDADES

1. Organización.
2. Procesos y procedimientos.
3. Personal
4. Ambiente físico
5. Configuración del sistema de información.
6. Hardware, software y equipos de comunicaciones.
7. Dependencia de partes externas.

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión
	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 de “terminación de sesión” cuando se abandona la estación de trabajo	Error en el uso
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Error en la disposición final de los medios
	Ausencias de pistas de auditoria	Error en el software
	Asignación errada de los derechos de acceso	Error en la asignación de perfiles
	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
	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 eficaz	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
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas	Espionaje remoto
RED	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
	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Daño de equipos y medios
	Inducción 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
PERSONAL	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
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Abuso de los derechos
	Ubicación en área susceptible de inundación	Abuso de los derechos
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	
	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
ORGANIZACIÓN	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 administradores y operadores	Abuso de los derechos
	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 la prestación de los servicios

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
	Ausencia de procedimientos de control de cambios	Errores de Uso
	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 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 mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

9 IDENTIFICACIONES DE CONTROLES

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	**Objetivo**: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos de la organización y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad y privacidad de la información.	**Control:** Manual de buenas prácticas y de la política de seguridad y privacidad de la información, aprobada por la dirección, publicado y comunicado a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad y privacidad de la información.	**Control:** Revisión de las políticas para seguridad y privacidad de la información las cuales se deben revisar periódicamente o cuando ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6.1	Organización interna	**Objetivo**: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información	**Control:** Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.2.1	Política para dispositivos móviles	**Control:** Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles
A.7.1	Antes de asumir el empleo	**Objetivo**: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.2	Términos y condiciones del empleo	**Control:** Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**Control**: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.8.1	Responsabilidad por los activos	**Objetivo**: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas
A.8.1.1	Inventario de activos	**Control**: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.8.2.1	Clasificación de la información	**Control**: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada
A.8.3.2	Disposición de los medios	**Control**: Se deben disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales
A.9.1	Requisitos de la organización para control de acceso	**Objetivo**: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	**Control**: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos de la organización y de seguridad de la información
A.9.1.2	Política sobre el uso de los servicios de red	**Control:** Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios	**Objetivo**: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios	**Control**: Se debe implementar un protocolo formal para el registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control**: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.6	Retiro o ajuste de los derechos de acceso	**Control**: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios
A.9.4.1	Restricción de acceso Información	**Control**: El acceso a la información y a las funciones de los sistemas de las aplicaciones se deben restringir de acuerdo con la política de control de acceso
A.9.4.3	Sistema de gestión de contraseñas	**Control**: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones
A.9.4.5	Control de acceso a códigos fuente de programas	**Control**: Se debe restringir el acceso a los códigos fuente de los programas.
A.10.1	Controles criptográficos	**Objetivo**: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos	**Control**: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.11.1	Áreas seguras	**Objetivo**: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización
A.11.1 1	Perímetro de seguridad física	**Control**: Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información
A.11.1 2	Controles físicos de entrada	**Control**: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado
A.11.1 4	Protección contra amenazas externas y ambientales	**Control**: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.2	Equipos	**Objetivo**: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos	**Control**: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	**Control**: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro
A.11.2.4	Mantenimiento de equipos	**Control**: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas
A.11.2.5	Retiro de activos	**Control**: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**Control**: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones
A.11.2.7	Disposición segura o reutilización de equipos	**Control**: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización
A.11.2.9	Política de escritorio limpio y pantalla limpia	**Control**: Se deben adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12.1	Procedimientos operacionales y responsabilidades	**Objetivo**: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.12.1.1	Procedimientos de operación documentados	**Control**: Los procedimientos de operación se debe documentar y poner a disposición de todos los usuarios que los necesiten
A.12.1.2	Gestión de cambios	**Control**: Se deberían controlar los cambios en la organización, en los procesos de organización, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
A.12.2	Protección contra códigos maliciosos	**Objetivo**: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	**Control**: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo	**Objetivo**: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información	**Control**: Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada
A.12.4	Registro y seguimiento	**Objetivo**: Registrar eventos y generar evidencia.
A.12.4.4	sincronización de relojes	**Control**: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo
A.12.5	Control de software operacional	**Objetivo**: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	**Control**: Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos
A.12.6	Gestión de la vulnerabilidad técnica	**Objetivo**: Prevenir el aprovechamiento de las vulnerabilidades técnicas
A.12.6.2	Restricciones sobre la instalación de software	**Control**: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales
A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de la organización
A.13.1	Gestión de la seguridad de las redes	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.13.1.2	Seguridad de los servicios de red	**Control**: Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente
A.13.1.3	Separación en las redes	**Control**: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes
A.13.2	Transferencia de información	**Objetivo**: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa
A.13.2.1	Políticas y procedimientos de transferencia de información	**Control**: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	**Control**: Los acuerdos deberían tener en cuenta la transferencia segura de información de la organización entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	**Control**: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**Control**: Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.15.1	Seguridad de la información en las relaciones con los proveedores	**Objetivo**: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**Control**: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	**Objetivo**: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.2	Reporte de eventos de seguridad de la información	**Control**: Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible
A.16.1.3	Reporte de debilidades de seguridad de la información	**Control**: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**Control**: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información
A.16.1.5	Respuesta a incidentes de seguridad de la información	**Control**: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**Control**: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros
A.17.1	Continuidad de seguridad de la información	**Objetivo**: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de organización de la organización
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**Control**: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.*
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Control**: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas
A.18.1	Cumplimiento de requisitos legales y contractuales	**Objetivo**: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.2	Derechos de propiedad intelectual	**Control**: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados
A.18.1.4	Privacidad y protección de datos personales	**Control**: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes

10 IDENTIFICACION DE RIESGOS DE LA INFORMACION PARA PASTO SALUD ESE

No	RIESGOS	VALORACION SEVERIDAD DEL RIESGO ANTES DE CONTROLES				VALORACION SEVERIDAD DEL RIESGO DESPUES DE CONTROLES				Priorización
		Activo	Probabilidad de Ocurrencia (inherente)	Impacto Inherente	Severidad	No de controles aplicado	Probabilidad con controles	Impacto con controles	Nivel	
R1	Posibilidad de perder completitud, la exactitud y la coherencia de datos de las bases de datos por modificaciones no autorizadas y vulneración de datos reservados debido a contraseñas no seguras, ausencia de mecanismos de autenticación, ausencia de bloqueos de sesión y ausencia de políticas de control de acceso.	Bases de datos	80%	80%	ALTO	5	4%	80%	ALTO	SI
R2	Posibilidad de pérdida de la confidencialidad y disponibilidad de la información por falla de los equipos de cómputo, mal funcionamiento de los equipos e infección por virus informático, debido a mantenimiento insuficiente, ausencia de reposición tecnológica, falta de equipos de refrigeración y/o inconvenientes por humedad, polvo o suciedad, descarga y uso no controlado de software y ausencia de virus.	Servidores Computadores de escritorio y portátiles Unidad NAS de almacenamiento	100%	80%	ALTO	7	4%	80%	ALTO	SI
R3	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por falla de la conectividad, falla de las telecomunicaciones y espionaje remoto. Debido a la ausencia de cumplimiento de los niveles de servicio por parte del proveedor, ausencia de equipos para la protección externa y conexiones de red sin protección.	Switches Acces Point Cableado Fibra Óptica Cableado Estructurado Fortigate	100%	80%	ALTO	3	22%	80%	ALTO	SI
R4	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por error en el uso de equipos y software, abuso de derechos, entrega equivocada de información, divulgación de contraseñas, revelación de información y fuga de	Personal Técnico Interno Personal Técnico Externo Colaboradores	80%	80%	ALTO	2	29%	80%	ALTO	SI

No	RIESGOS	VALORACION SEVERIDAD DEL RIESGO ANTES DE CONTROLES				VALORACION SEVERIDAD DEL RIESGO DESPUES DE CONTROLES				Priorización
		Activo	Probabilidad de Ocurrencia (inherente)	Impacto Inherente	Severidad	No de controles aplicado	Probabilidad con controles	Impacto con controles	Nivel	
	información. Debido a entrenamiento insuficiente, desconocimiento y falta de apropiación de la política de seguridad de la información, desconocimiento en los tiempos de entrega y recepción de documentos.									
R5	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por copia fraudulenta de software, infección por virus informático, falla de los sistemas de información, errores de software, instalaciones y uso no autorizado de software. Debido a descarga y uso no controlado de software, ausencia de copias de respaldo, ausencia de antivirus, ausencia de validación de licenciamiento, mantenimiento insuficiente y ausencia de políticas de restricción de software.	Sistema de Información SIOS Sistema ORFEO Sistema de Costos Antivirus MilPS Infomedic Spark Ostickets Sistemas Operativos Windows Office Bussines	100%	100%	EXTREMO	6	13%	65%	MODERADO	SI
R6	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por fuga de información, inundaciones y pérdida de información. Debido a la ausencia de controles de acceso físico, susceptibilidad a la humedad, el polvo y la suciedad y falta de copias de respaldo.	Archivos electrónicos y digitales Documentos físicos y comunicaciones oficiales	80%	80%	ALTO	5	4%	80%	ALTO	SI
R7	Posibilidad de afectación de credibilidad e imagen institucional por la desinformación a los grupos de interés, Debido a difusión de noticias falsas, información incompleta entregada por la Empresa, inoportunidad en la entrega de la información, ausencia de medios y canales de comunicación	Piezas audiovisuales: Videos, Post, Banners, Comunicados de presa, programas radiales. Afiches	80%	60%	ALTO	3	17%	60%	MODERADO	SI

11 TRATAMIENTO DE RIESGOS

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9

MATRIZ DE RIESGOS - SEGURIDAD DE LA INFORMACION (PARTE B)

VERSION	PROCESO / SERVICIO	CODIGO	NUM
6,0	GESTION DE SISTEMAS DE INFORMACION	GSI-RSI	411-B

FECHA DE ACTUALIZACION:	2024	MACROPROCESO	PROCESO SISTEMAS DE INFORMACION

PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACIÓN DEL RIESGO SIN CONTROLES			CONTROLES	VALORACIÓN DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
																		INICIO	FINAL	
GESTION DE SISTEMAS DE INFORMACION	**R1 Posibilidad de** perder completitud, exactitud y la coherencia de datos de las bases de datos **por** modificaciones no autorizadas y vulneración de datos reservados **debido a** contraseñas no seguras, ausencia de mecanismos de autenticación, ausencia de bloqueos de sesión y ausencia de políticas de control de acceso.	Bases de datos	INFORMACION	.Modificaciones no autorizadas .Vulneración de datos reservados	**V1**.Contraseñas no seguras **V2**.Ausencia de mecanismos de autenticación de usuarios **V3**.Ausencia de bloqueos de sesión **V4**.Ausencia de políticas de control de acceso	.Legales .Económicas .Inadecuada toma de decisiones .Error en la recepción y envío de comunicaciones oficiales . Afectación de la imagen y reputación	ALTO	80% Alta	80% Mayor	ALTO	**Control 1: (V4)** El ingeniero de sistemas encargado de realizar la auditoría de seguridad de la información, verifica que los colaboradores estén aplicando las buenas prácticas de seguridad y privacidad de la información, a través de una evaluación de conocimientos y de un cuestionario de verificación en los puestos de trabajo de las sedes auditadas. **Control 2: (V2)**El Sistema de gestión de base de datos relacional SQL Server verifica que los roles y derecho de acceso de los usuarios sean los correctos para el acceso a las bases de datos a través del inicio de sesión del usuario y contraseña asignados. **Control 3: (V3)**El administrador de directiva de grupos del directorio activo de manera automática bloquea los usuarios que han intentado acceder más de tres veces con la contraseña errónea a través de la política del directorio activo implementado. **Control 4: (V1)**El administrador de directiva de grupos del directorio activo de manera automática valida que las contraseñas creada contengan combinación de mínimo 8 caracteres través de la política de contraseñas seguras del directorio activo implementado. **Control 5: (V2)**. Asignación de perfiles a las bases de datos por custodios de la información y seguimiento.	4% Muy baja	80% Mayor	ALTO	**MITIGAR EL RIESGO** (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es muy baja de acuerdo a los controles preventivos aplicados en la Entidad)	1. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. Líder del proceso Oficina Control Interno	**Semestralmente**		**Control 1:** Informe de seguimiento a buenas prácticas de seguridad de la información por parte del ingeniero de sistemas. **Control 2:** Demostración en vivo por parte del profesional Universitario. **Control 3:** Demostración en vivo por parte del profesional Universitario. **Control 4:** Demostración en vivo por parte del profesional Universitario. **Control 5:** Demostración en vivo por parte del profesional Universitario.

GESTION DE SISTEMAS DE INFORMACION	**R3** **Posibilidad de** pérdida de confidencialidad y disponibilidad de la información **por** falla de la conectividad, falla de las telecomunicaciones y espionaje remoto, **debido** a la ausencia de cumplimiento de los niveles de servicio por parte del proveedor, ausencia de equipos para la protección externa y conexiones de red sin protección.	. Switches . Acces Point . Cableado Fibra Óptica . Cableado Estructurado . Fortigate	REDES	. Falla de la conectividad . Falla de las telecomunicaciones . Espionaje Remoto (Hackers)	**V1**. Ausencia de cumplimiento de los niveles de servicio por parte de proveedor. **V2**. Ausencia de equipos para la protección externa **V3**. Conexiones de red sin protección	. Pérdida de la información durante la contingencia (Historia Clínica). . Perdida de tiempo operacional . Perdida de datos al momento de la caída del servicio	ALTA	100% Muy Alta	80% Mayor	ALTO	**Control 1: (V1)** El jefe la Oficina Asesora de Comunicaciones y Sistema verifica el cumplimiento del servicio de conectividad e internet a través del acuerdo de nivel de servicios establecido en el contrato con el proveedor. **Control 2: (V1)** La herramienta PRTG monitorea los niveles de servicios de conectividad e internet a través del indicador del informe mensual suministrado por el software donde se establecen las caídas de los servicios. **Control 3: (V2,V3)** El equipo Firewall es un dispositivo de seguridad perimetral que controla amenazas emergentes detectando prevención de intrusos, bloqueo a sitios web maliciosos, amenazas de malware a través del firewall.	22% Baja	80% Mayor	ALTO	**MITIGAR EL RIESGO**	1.Solicitar al proveedor las vulnerabilidades de software malicioso presentadas y las acciones de mitigación implementadas en Firewall 2. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. Jefe oficina sistemas de información 2. Líder del proceso Oficina Control Interno	1. 1/07/2024 2. Semestralmente	1. 31/12/2024	**Control 1**: Informe de seguimiento a la prestación del servicio de conectividad,internet y seguridad perimetral por parte del supervisor del contrato. **Control 2:** Demostración en vivo por parte del ingeniero de sistemas a cargo del seguimiento y monitoreo de la herramienta PRTG. **Control 3:** Demostración en vivo por parte del proveedor quien administra el firewall.
GESTION DE SISTEMAS DE INFORMACION	**R4** **Posibilidad de pérdida** de confidencialidad y disponibilidad de la información **por error** en el uso de equipos y software, abuso de derechos, entrega equivocada de información, divulgación de contraseñas, revelación de información y fuga de información. **Debido a** entrenamiento insuficiente, desconocimiento y falta de apropiación de la política de seguridad de la información, desconocimiento en gestión documental y uso de la herramienta de sistemas de información documental.	. Personal Técnico Interno . Personal Técnico Externo . Colaboradores	TALENTO HUMANO	. Error en el uso de equipos y software . Abuso de derechos . Entrega equivocada de correspondencia . Divulgación de contraseñas. . Revelación de información. . Fuga de información.	**V1**. Entrenamiento insuficiente **V2**. Desconocimiento y Falta de apropiación de la política de seguridad de la información **V3**. Desconocimiento en gestión documental y uso de la herramienta de sistemas de información documental	.Sanciones disciplinarias .Legales .Económicas . Imagen Reputación	ALTA	80% Alta	80% Mayor	ALTO	**Control 1: (V1,V2)** El ingeniero de sistemas elabora la capacitación virtual para el conocimiento y aplicabilidad de la política de seguridad de la información para personal interno, a través de un cuestionario de evaluación en la plataforma Moodle. **Control 2: (V3)** La Dependencia de Gestión Documental realiza capacitación a todos los trabajadores para el manejo de la conservación documental, tablas de retención documental y software para sistemas de información documental	29% Baja	80% Mayor	ALTO	**MITIGAR EL RIESGO**	1. Sensibilizar a los a colaboradores de la entidad en la apropiación de la política de seguridad de información, manual de política de seguridad de la información. 2. Realizar capacitaciones cortas y concretas al respecto, en el manejo sensible de la información y comunicaciones evitando que los colaboradores incurra en errores de tipo procedimental por desconocimiento. 3. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. y 2. Ingeniero de Sistemas Técnicos de Sistemas Técnico Archivo 3. Líder del proceso Oficina Control Interno	1. y 2. 1/07/2024 3. Semestralmente	1. y 2. 31/12/2024	**Control 1:** Informe de capacitación en seguridad de la información al personal interno en la plataforma Moodle por parte del responsable de la actividad. **Control 2:** Inofrme y registro de asistencia de las capcitaciones en gestion documental al personal interno por parte de la Tecnico Administrativo Gestión Docuemntal.

GESTION DE SISTEMAS DE INFORMACION	**R5 Posibilidad de** pérdida de confidencialidad y disponibilidad de la información **por** copia fraudulenta de software, infección por virus informático, falla de los sistemas de información, errores de software, instalaciones y uso no autorizado de software, **debido a** descarga y uso no controlado de software, ausencia de copias de respaldo, ausencia de antivirus, ausencia de validación de licenciamiento, mantenimiento insuficiente y ausencia de políticas de restricción de software.	. Sistema de Información SIOS . Sistema ORFEO . Sistema de Costos . Antivirus . MIPS . Infomedic . Spark . Ostickets . Sistemas Operativos Windows . Office Bussines	SOFTWARE	. Copia Fraudulenta de Software . Infección por virus informático (Spyware/Malware) . Fallo de los sistemas de información . Infracción legal . Errores de software. . Instalación no autorizada de software. . Uso no autorizado de software.	**V1**.Descarga y uso no controlado de software **V2**. Ausencia de copias de respaldo **V3**. Ausencia de antivirus **V4**. Ausencia de validación de licenciamiento **V5**. Mantenimiento insuficiente **V6**. Ausencia de políticas de restricción de software	.Legales .Económicas .No continuidad en el proceso de atención integral en salud y procesos de apoyo a través de la herramienta SIOS . Subfacturación por no disponibilidad del sistema SIOS	MEDIA	100% Muy Alta	100% Catastrofico	EXTREMO	**Control 1: (V1)** El directorio activo de Windows server tiene configuradas las políticas de seguridad de la información a nivel de software que controlan las descargas e instalación de software no autorizados a los recursos informáticos a través de alertas como acciones preventivas. **Control 2: (V2)** Microsoft SQL Server es un motor de base de datos que ejecuta las copias de respaldo de las bases de datos y archivos de los servidores y equipos a través de la programación de copias de respaldo full y diferenciales programadas. **Control 3: (V3)** El sistema de antivirus implementado detecta, evita y elimina malware comparando cada archivo del disco duro con un diccionario de virus ya conocidos. Si cualquier pieza de código en un archivo del disco duro coincide con el virus conocido en el diccionario, el software antivirus entra en acción, llevando a cabo una de las acciones posibles. **Control 4: (V4)** El supervisor de los contratos de compra venta de licencias de software verifica la adquisición y activación de las mismas a través de la plataforma del fabricante y/o certificación por parte del partner. **Control 5: (V5)** El supervisor del contrato de mantenimiento preventivo y correctivo de equipos de comunicaciones y sistemas verifica que se haya ejecutado el mantenimiento por parte del contratista a través del informe que envía el proveedor y la firma del registro a satisfacción de los mantenimientos por parte de los técnicos de sistemas. **Control 6: (V6)** EL directorio activo de Windows server tiene configuradas las políticas de seguridad de la información a nivel de software que controlan los accesos a la red de datos y validan usuarios y contraseñas a través de los perfiles asignados a los colaboradores	13% Muy Baja	65% Mayor	MODERADO	**MITIGAR EL RIESGO**	1. Solicitar al proveedor las vulnerabilidades de software malicioso presentadas y las acciones de mitigación implementadas en Firewall 2. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1Profesional Universitario Sistemas 2. Líder del proceso Oficina Control Interno	1. 1/07/2024 2. Semestralmente	1. 31/12/2024	**Control 1:** Demostración en vivo por parte del profesional Universitario. **Control 2:** Demostración en vivo por parte del profesional Universitario. **Control 3:** Verificación en sitio de intalación de antivirus en los equipos de computo por parte del técnico se sistemas en todas las sedes. **Control 4**: Demostración en vivo por parte del jefe de la Oficina Asesora de Comunicaciones y Sistemas o del Profesional delegado. **Control 5:** Informe de seguimiento a mantenimineto preventivo y correctivo por parte del supervisor del contrato. **Control 6:** Demostración en vivo por parte del profesional Universitario.

GESTION DE SISTEMAS DE INFORMACION	**R6** **Posibilidad de** pérdida de confidencialidad y disponibilidad de la información **por** fuga de información, inundaciones y perdida de información. **Debido a** la ausencia de controles de acceso físico, susceptibilidad a la humedad, el polvo y la suciedad y falta de copias de respaldo.	. Archivos electrónicos y digitales . Documentos físicos y comunicaciones oficiales	INFORMACION	. Fuga de información . Inundaciones . Perdida de información	**V1** Ausencia de Controles de acceso físico **V2.** Susceptibilidad a la humedad el polvo y la suciedad **V3.** Falta de copias de respaldo	. Legales .Económicas . Imagen Reputación	ALTA	80% Alta	80% Mayor	ALTO	**Control 1: (V2)** El dispositivo termo higrómetro mide la temperatura y humedad de los archivos de historia clínica, a través del formato de registro definido para tal fin se llevan los datos históricos de la medición. **Control 2: (V2)** El personal de aseo realiza limpieza y desinfección de las áreas de archivo y registra en el formato de limpieza y desinfección estandarizado por la empresa **Control 3: (V1)** El profesional Universitarios de Salud y Seguridad en el trabajo implementó la señalización a los espacios físicos de los archivos, data center y oficinas de la empresa mediante avisos preventivos de acceso al personal interno y externo. **Control 4: (V1)** El jefe de la oficina Asesora de comunicaciones y Sistemas gestionó la instalación de una puerta electrónica con clave de acceso al datacenter de la empresa, la clave de acceso es manejada solo por el personal de ingenieros de la oficina. **Control 5: (V1)** Cámaras de video vigilancia instaladas en algunas Sedes de Pasto Salud permite controlar el acceso a los sitiod de las diferentes sedes través de las grabaciones realizadas en el DVR.	4% Muy Baja	80% Mayor	ALTO	**MITIGAR EL RIESGO**	1. Verificación semestral del cumplimiento de las actividades propuestas en el documento sistema integrado de conservación SIC 2. Se valida mensualmente que los usuarios realicen la copia de seguridad en el espacio asignado en la unidad de almacenamiento del datacenter. Se lleva un registro de que usuarios realizaron copia y quienes no, con el fin de recordar a los usuarios de la importancia de las copias de seguridad y evitar perdidas de información. 3. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. y 2. Profesional Universitario Sistemas 2. Técnico de sistemas 3. Líder del proceso Oficina Control Interno	1.y 2 M07/2024 3. Semestralmente	1. y 2.31/12/2024	**Control 1:** Verificación en sitio donde están instalados los termo higrómetros. **Control 2:** Registros de limpieza y desinfección entregados por parte de la Tecnico Administrativo de Gestión Documental. **Control 3:** Verificación en sitio donde están instalados los avisos de advertencia de accesos restringidos. **Control 4:** Verificación en el Data Center de la puerta de Seguridd con clave de acceso. **Control 5:** Verificación en sitio de las camaras de Seguridad.
STEMAS DE INFORMACION	**R7** **Posibilidad de** afectación de credibilidad e imagen institucional **por** la desinformación a los grupos de interés, **Debido a** difusión de noticias falsas, información incompleta entregada por la Empresa, inoportunidad en la entrega de la información, ausencia de medios y canales de comunicación	. Piezas audiovisuales: Videos, Post, Banners, Comunicados de prensa, programas radiales. Afiches.	INFORMACION	Desinformación a los grupos de interés	**V1:** Difusión de noticias falsas **V2** Información incompleta entregada por la Empresa **V3:** Inoportunidad en la entrega de la información **V4:** Ausencia de medios y canales de comunicación (arreglar)	. Crisis comunicacional . Insatisfacción de las partes interesadas . Perdida de Reputación e Imagen . Perdidas económicas	ALTA	80% Alta	60% Moderado	ALTO	**Control 1: V1, V2:** El técnico operativo realiza la capacitación del protocolo de comunicación de crisis mediáticas, reputacional o informativa que permite a los funcionarios abordar situaciones de crisis comunicacional **Control 2: V4** La empresa, tiene implementados y adoptados canales de comunicación de manera oficial para asegurar la comunicación de la información institucional hacia las partes interesadas. **Control 3: V(1)** El grupo de comunicaciones, anualmente, realiza o actualiza la matriz de comunicaciones para brindar información institucional a las partes interesadas	17% Muy Baja	60% Moderado	MODERADO	**MITIGAR EL RIESGO**	1. Realizar el procedimiento para la estandarización de la entrega de información a las partes interesadas. 2. Socializar el procedimiento para la estandarización de la entrega de información a las partes interesadas a todo el personal de la entidad 3. Aplicar el procedimiento para la estandarización de la	1 y 2 Técnico operativo - Comunicaciones y sistemas 3. Todo el personal	1. Julio 2024 2. Septiembre 2024 3.		**Control 1:** **Control 2:** Verificación de los canles de comunicación. **Control 3:** Matriz de comunicaciones actualizada

12 MODELO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN – SGSI

13 PERSONAL DE SEGURIDAD DE LA INFORMACION

Las funciones del personal de seguridad de la información son asumidas por los profesionales Universitarios Sistemas de la Oficina asesora de Comunicaciones y Sistemas de Pasto Salud E.S.E.

14 IMPLEMENTACIÓN DEL PLAN DE ACCION DE TRATAMIENTO DE RIESGOS

El plan de implementación de tratamiento de riesgos, comprende las siguientes actividades, cronograma y recursos asignados:

EMPRESA SOCIAL DEL ESTADO
PASTO SALUD E.S.E
NIT.900091143-9

PLAN DE ACCION DE AREAS, OFICINAS Y/O DEPENDENCIAS

ION	PROCESO/SERVICIO	CODIGO	NUM
	DIRECCIONAMIENTO ESTRATEGICO	DE-PAA	013

OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS	VIGENCIA DEL PLAN DE ACCION: 2025	2025
	APROBACIÓN DEL PLAN DE ACCION	2025/01/27

FUNCIONES, ROLES O COMPETENCIAS	ACTIVIDADES / ACCIONES	# ACTIVIDADES	RESULTADO ESPERADO O IMPACTO	META	INDICADORES	EVIDENCIAS DOCUMENTALES	TIEMPO		RESPONSABLE
							INICIA	TERMINA	
Diseñar y administrar el Plan de Seguridad Informática y de la información institucional a fin de garantizar, la integridad, la Confidencialidad y disponibilidad de la información.	Revisión y actualización de la matriz de riesgos	1	Fortalecimiento de la gestión integral de riesgos de la organización, permitiendo identificar, evaluar, mitigar y monitorear amenazas de manera proactiva, lo que asegura la continuidad operativa, mejora la toma de decisiones estratégicas y fomenta una cultura de mejora continua y resiliencia organizacional.	>=95%	Solicitud de Gestión de Incidentes de seguridad de la información resueltos	Matriz de riesgos actualizada	Enero 2025	Enero 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Equipo Oficina Comunicaciones y Sistemas
	Socialización de la matriz de Riesgos y Plan de tratamiento de riesgos al equipo de la Oficina Asesora de Comunicaciones y Sistemas	1				Acta y Registro de asistencia a la socialización al equipo de la Oficina Asesora de Comunicaciones y Sistemas	Enero 2025	Febrero 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas / Profesional Universitario
	Seguimiento de controles aplicados a los riesgos	1			Efectividad para mitigar el riesgo de perdida de la información por ataques de software malicioso y virus informático	Informe de seguimiento y evaluación trimestral	Febrero 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Equipo Oficina Comunicaciones y Sistemas
	Evaluación de la efectividad de los controles	1					Abril 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Equipo Oficina Comunicaciones y Sistemas
	Identificar oportunidades de mejora frente a los resultados no esperados.	1				Actividades de mejora	Abril 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Equipo Oficina Comunicaciones y Sistemas
Observaciones a la acción/actividad:	Cuando sea necesario incluir observaciones para la acción/actividad formulada, inserte la fila de observaciones después de cada actividad. Para ello seleccione la fila desde la barra de numeración, de clic derecho y seleccione la orden copiar, ubíquese en la fila siguiente a la de acción/actividad descrita sobre la cual tiene observaciones, con clic derecho de seleccione la orden **insertar celdas copiadas.**								
OTRAS ACTIVIDADES DE COMPETENCIA A LA OFICINA / DEPENDENCIA (Corresponde a aquellas que no tienen relación directa con las funciones de la Dependencia u Oficina a cargo y que no son contradictorias a su competencia, ni extralimitan sus funciones)									

Insertar las filas que sean necesarias, o eliminar aquellas que sobren al diligenciar la matriz del Plan de Acción.

ELABORÓ:	REVISÓ:	APROBÓ:
WILLIAM RICARDO MONTENEGRO GUEVARA Profesional Universitario Oficina Asesora Comunicaciones y Sistemas	LYDA ARGELIS PABON LOPEZ Jefe Oficina Asesora Comunicaciones y Sistemas	DIEGO FERNANDO MORALES ORTEGON Gerente

BIBLIOGRAFÍA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por 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 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo 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.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 1008 del 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.
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital

Fin del documento.

ACTUALIZADO POR:

WILLIAM RICARDO MONTENEGRO GUEVARA
Profesional Universitario

REVISADO POR:

LYDA ARGELIS PABÓN LOPEZ
Jefe Oficina Asesora de Comunicaciones y Sistemas

APROBADO POR:

DIEGO FERNANDO MORALES ORTEGÓN
Gerente