EMPRESA SOCIAL DEL ESTADO

PASTO SALUD E.S.E

NIT.900091143-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN 9.0

SAN JUAN DE PASTO
2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
PASTO SALUD E.S.E.

ACTUALIZO

WILLIAM MONTENEGRO GUEVARA
Profesional Universitario

SAN JUAN DE PASTO
2025

TABLA DE CONTENIDO

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

SOLICITUD DE CREACIÓN, MODIFICACION Ó ELIMINACION DE DOCUMENTOS Y REGISTROS			
VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
8.0	GESTION DE SISTEMAS DE INFORMACION	GSI-MDR	225

PROCESO	PROCEDIMIENTO		TIPO DE DOCUMENTO	
GESTION DE SISTEMAS DE INFORMACION	GESTION DE SISTEMAS DE INFORMACION		. PLAN	
NOMBRE DEL DOCUMENTO		CODIGO	FECHA	TIPO DE SOLICITUD
PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION		MA- PSII	27 de enero de 2025	MODIFICACION/ACTUALIZACION
CAUSAS DE (Creación, Modificación o eliminación)	Actualización del plan para la vigencia 2025			
DESCRIPCION DE LAS MEJORAS	Resolución, Plan de acción vigencia 2025 y Politica de Seguridad de la Información			
SECCIÓN MODIFICADA AL DOCUMENTO	8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8.1 IDENTIFICAR, CLASIFICAR, Y ACTUALIZAR LOS ACTIVOS DE LA INFORMACIÓN DE LA EMPRESA 8.2 SENSIBILIZAR AL TALENTO HUMANO EN LAS MEJORES PRÁCTICAS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 8.3 FORTALECER LOS MECANISMOS DE RESPALDO DE LA INFORMACIÓN FÍSICA COMO DIGITAL PARA SU PRESERVACIÓN Y CONSERVACIÓN. 8.4 GESTIONAR LOS INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		ACEPTADO SI NO	
NOMBRES Y APELLIDOS DE QUIEN ELABORÓ	NOMBRES Y APELLIDOS DE QUIEN REVISÓ (Líder de proceso o jefe inmediato de acuerdo a la estructura organizacional de la empresa)		NOMBRES Y APELLIDOS DEL (LA) GERENTE-APRUEBA	
WILLIAM MONTENEGRO GUEVARA	LYDA PABÓN LOPEZ		DIEGO FERENANDO MORALES ORTEGÓN	
CARGO PROFESIONAL UNIVERSITARIO	CARGO JEFE OFICINA		CARGO GERENTE	
FIRMA	FIRMA		FIRMA	

EL PRESENTE FORMATO ES IDENTICO AL ORIGINAL APROBADO, LAS MODIFICACIONES AL FORMATO NO SON VÁLIDAS SIN APROBACIÓN (FIRMAS EN FORMATO ORIGINAL), OFICINA ASESORA DE PLANEACIÓN, FECHA DE CREACION Y/O ACTUALIZACION: 22-11-2022

VIGILADO Supersalud

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	
9.0	Actualización Plan de Seguridad y Privacidad de la Información.		X		**Justificación**: Se realiza actualización plan vigencia 2025.	Equipo Oficina Asesora de Comunicaciones y Sistemas William Montenegro Guevara – Profesional Universitario José Fernando Mora Montenegro - Contratista	Formato 225 de creación, modificación o eliminación de documentos y registros del 27 de enero de 2025 Resolución 088 del 27 de enero de 2025
8.0	Actualización Plan de Seguridad y Privacidad de la Información.		X		**Justificación**: Se realiza actualización plan vigencia 2024	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 060-28-01-2021
7.0	Actualización Plan de Seguridad y Privacidad de la Información.		X		**Justificación**: Se realiza ajuste a la política de Seguridad de la Información, Se ingresó un objetivo específico, se modificó el Modelo y Operación del Sistema de Seguridad de la Información.	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 060-28-01-2021
6.0	Elaboración y aprobación del Plan de Seguridad y Privacidad de la Información.	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 092 del 29 de enero de 2020

INTRODUCCIÓN

La Empresa Social del Estado Pasto Salud E.S.E. tiene como misión brindar servicios de atención primaria y complementaria en salud en el municipio de Pasto, a través de sedes integradas en red con un enfoque preventivo, predictivo y resolutivo. Buscamos asegurar que cada proceso sea realizado de manera segura, humanizada y efectiva, con un equipo comprometido, garantizando el uso eficiente de los recursos tecnológicos y financieros para satisfacer las necesidades y expectativas de nuestros grupos de interés. En este contexto, la mejora continua de la calidad de nuestros servicios es de suma importancia para lograr la excelencia en la atención.

Así las cosas, la información se considera como uno de los activos más importantes y valiosos de nuestra empresa, siendo un recurso indispensable para el desarrollo y cumplimiento de nuestra misión. Dado que la información es sensible o crítica, es importante determinar el nivel de protección necesario para mitigar los riesgos asociados a la pérdida de su disponibilidad, integridad o confidencialidad. Una gestión adecuada y segura de la información no solo garantiza el éxito de nuestras operaciones, sino también la confianza de nuestros grupos de interés y el cumplimiento de las normativas vigentes.

Siguiendo las directrices establecidas en materia de seguridad digital y de la información, y en concordancia con el Decreto 1008 de 2018, la Empresa Social del Estado Pasto Salud E.S.E. adopta como principio fundamental la seguridad de la información, según lo dispuesto en el artículo 2.2.9.1.1.3 de la normativa mencionada. Asimismo, el artículo 2.2.9.1.2.1 establece la estructura de los componentes y habilitadores transversales de la Política de Gobierno Digital, tales como los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que son clave para el desarrollo de los componentes y el logro de los objetivos de la Política.

En este marco, se ha formulado el Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud E.S.E., buscando fortalecer la protección de los datos e información, garantizando su confidencialidad, integridad y disponibilidad en todos los procesos. Este plan está enfocado en alcanzar y mantener una cultura y conciencia en el acceso y uso adecuado de la información.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Establecer los lineamientos necesarios para la protección de los activos de información y el uso adecuado de los mismos, con el fin de preservar su disponibilidad, integridad y confidencialidad.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar, clasificar, y actualizar los activos de la información de la empresa.

- Sensibilizar al talento humano en las mejores prácticas de la seguridad y privacidad de la información.

- Fortalecer los mecanismos de respaldo de la información física como digital para su preservación y conservación.

- Limitar la pérdida de datos y gestionar los incidentes de recuperación de la información para mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Aplica a todas las sedes de Pasto Salud E.S.E, a todos sus grupos de interés, funcionarios, contratistas y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de Pasto Salud E.S.E generen, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

Así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación.

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

Ley 1273 de 5 de enero 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.

Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Ley Estatutaria 1266 de 2008. Por la cual se dictan las disposiciones generales de 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. Para conocer más de esta Ley,

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Resolución No. 00500 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.

Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

5. GLOSARIO

Amenaza: es el conjunto de los peligros a los que están expuestos los sistemas de información y sus recursos tecnológicos relacionados, los que pueden ser de tipo accidental o intencional.

Amenaza accidental: cuando no existe un deliberado intento de perjudicar a la organización.

Amenaza intencional: su móvil es perjudicar a la organización u obtener beneficios en favor de quien comete la acción.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Confidencialidad: asegurar que los sistemas de información y sus recursos relacionados sean solo accedidos por los funcionarios o contratistas de Pasto Salud E.S.E, basados en la necesidad de saber o de hacer de sus cargos.

Disponibilidad: asegurar que los usuarios autorizados tienen acceso a los sistemas de información y sus recursos relacionados, en tiempo y forma, cuando sean requeridos.

Integridad: exactitud y plenitud de los sistemas de información y sus recursos relacionados, limitando la gestión sobre los mismos a personas autorizados y programas de aplicación aprobados y autorizados, protegiéndolos contra pérdida, destrucción o modificaciones accidentales o intencionales.

Información: puede existir en muchas formas. Puede estar impresa en papel, almacenada electrónicamente, transmitida por correo electrónico o utilizando medios magnéticos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Hacker: usuario de computadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta y en algunos casos provocar daños.

Keylogger: es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Phishing: es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc.

Política: son instrucciones mandatorios que indican la intención de la alta gerencia respecto a la operación de la organización respecto a un asunto determinado.

Privacidad: evitar que trascienda a terceras personas información de Pasto Salud E.S.E., referida a individuos, protegiendo a los mismos contra la divulgación indebida de su información personal y protegiendo la responsabilidad de la empresa sobre este tipo de divulgaciones.

Procesos informáticos: son los procesos que tienen relación directa con los servicios que se prestan a los usuarios de los sistemas de información y sus tecnologías relacionadas, procesos que consisten en tomar un insumo, agregarle valor y generar un producto que satisface a un cliente interno o externo.

Recurso Informático: elementos informáticos (base de datos, sistemas operacionales, redes, equipos de cómputo, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Seguridad de la Información: se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. (ISO27001).

Sniffer: es un software que permite capturar tramas de la red. Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas, etc.

Usuarios Terceros: todas aquellas personas naturales o jurídicas, que no son funcionarios o contratistas de Pasto Salud ESE, pero que por las actividades que realizan en la Entidad, deban tener acceso a recursos informáticos.

TI: tecnología de la información.

6. MODELO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN – SGSI

Pasto Salud ESE, adopta el Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, el cual protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

7. PERSONAL DE SEGURIDAD DE LA INFORMACIÓN

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

- Ing. Christian Muñoz De La Rosa - Profesional Universitario
- Ing. José Fernando Mora Montenegro – Contratista
- Ing. William Ricardo Montenegro Guevara - Profesional Universitario

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de implementación para el componente de seguridad y privacidad de la información, comprende las siguientes estrategias definidas en los siguientes planes de acción, de acuerdo a los objetivos planteados:

8.1 IDENTIFICAR, CLASIFICAR, Y ACTUALIZAR LOS ACTIVOS DE LA INFORMACIÓN DE LA EMPRESAÇ

La identificación, clasificación y actualización de los activos de información hacen parte de la seguridad y privacidad de los datos. La realización del inventario y clasificación de activos hace parte de la debida diligencia establecida a nivel estratégico en el Modelo de Seguridad y Privacidad de la Información, con el fin de asegurar la protección de los activos de información de los procesos. Mantener un inventario actualizado de los activos permite identificar los riesgos asociados, aplicar las medidas de seguridad adecuadas y asegurar la continuidad y confiabilidad de la información en la empresa.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	PLAN DE ACCION DE AREAS, OFICINAS Y/O DEPENDENCIAS			
	VERSION	PROCESO/SERVICIO	CODIGO	NUM
	6,0	DIRECCIONAMIENTO ESTRATEGICO	DE-PAA	013

OFICINA ASESORA COMUNICACIONES Y SISTEMAS	VIGENCIA DEL PLAN DE ACCION	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	
Revisar y verificar los archivos de gestión documental producida en la E.S.E. Pasto Salud. Realizar capacitaciones a todo el personal de la E.S.E. Pasto Salud el sobre manejo de archivos teniendo en cuenta el ciclo vital del documento Revisar y verificar los archivos de gestión documental producida en la E.S.E. Pasto Salud.	Validar los activos de información en Formato GSI-IPA 257	1	Mejora la gestión de la información al garantizar un inventario actualizado y completo de activos, lo que optimiza la toma de decisiones, fortalece la seguridad y asegura el cumplimiento normativo en la organización.	>=80%	1. Tablas de Retención Documental aplicadas correctamente 2.Solicitudes de necesidades de información 3.Solicitudes de necesidades de información respondidas negativamente 4.Solicitudes de necesidades de información respondidas negativamente por inexistencia de información	Formato GSI-IPA 257 validado	Febrero 2025	Marzo 2025	Todo el personal con manejo de información
	Identificar nuevos activos de información en cada dependencia	2		>=80%		Formato GSI-IPA 257 actualizado	Abril 2025	Junio 2025	Líderes de procesos Técnico Administrativo Gestión Documental
	Consolidar, actualizar, validar y publicar los activos de información	3		>=80%		Formato GSI-IPA 257 publicado	Julio 2025	Julio 2026	Jefe Oficina Asesora Comunicaciones y Sistemas Técnico Administrativo Gestión Documental
	Realizar acciones de mejora	1		>=80%		Informe	Agosto 2025	Agosto 2025	Jefe Oficina Asesora Comunicaciones y Sistemas Personal con manejo de información
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:
ROSARIO VILLALBA HIDALGO Técnico Administrativo	LYDA ARGELIS PABON LOPEZ Jefe Oficina Asesora Comunicaciones y Sistemas	DIEGO FERNANDO MORALES ORTEGÓN Gerente

8.2 SENSIBILIZAR AL TALENTO HUMANO EN LAS MEJORES PRÁCTICAS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Implica promover un cambio cultural en la empresa, orientado a la protección de la información. No se trata solo de implementar tecnologías, sino de involucrar al talento humano en el manejo responsable de los datos, comprendiendo la importancia de su rol en la seguridad y privacidad de la información. Esta sensibilización ayuda a reducir riesgos, garantiza el cumplimiento de normativas y mejora la confianza de los pacientes en la protección de sus datos.

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

PLAN DE ACCION DE AREAS, OFICINAS Y/O DEPENDENCIAS

VERSION	PROCESO/SERVICIO	CODIGO	NUM
6,0	DIRECCIONAMIENTO ESTRATEGICO	DE-PAA	013

OFICINA ASESORA COMUNICACIONES Y SISTEMAS

VIGENCIA DEL PLAN DE ACCION	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	
Planificar y ejecutar el seguimiento a la política de seguridad de la información y planes de contingencia, con sus respectivas capacitaciones e informes. Socializar la Política de Seguridad de la Información al personal de la entidad haciendo uso de las herramientas tecnológicas	Planificar las temáticas de capacitación de seguridad de la información en el plan institucional de capacitaciones de la Entidad	1	Fortalece la cultura organizacional en seguridad de la información, minimiza riesgos asociados a incidentes de seguridad, asegura el cumplimiento de políticas y mejora la protección de los datos sensibles en los centros de salud.	100%	NA	Plan Institucional de Capacitaciones, Informe de capacitación	Febrero 2025	Abril 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Contratista Ingeniero de sistemas Oficina de Comunicaciones y Sistemas
	Elaborar cronograma de control y seguimiento a la política de seguridad de información en los centros de salud	2		100%	NA	Informe / acta de cronograma de visita crentro de salud	Febrero 2025	Junio 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Contratista Ingeniero de sistemas Oficina de Comunicaciones y Sistemas
	Ejecutar plan de capacitaciones de seguridad de la información y plan de contingencia en sistemas de información	1		80%	NA	Informe de resultados en tamaticas propuestas	Febrero 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Contratista Ingeniero de sistemas Oficina de Comunicaciones y Sistemas
	Ejecutar actividades de control y seguimiento de seguridad de la información en equipos de computo instalados en los centros de salud	1		70%	NA	Acta de seguimiento y control	Marzo 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Contratista Ingeniero de sistemas Oficina de Comunicaciones y Sistemas
	Evaluar las actividades realizadas durante el control y seguimiento se seguridad de la información en centros de salud	1		90%	NA	Acta de Evaluación y resultados	Agosto 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Contratista Ingeniero de sistemas Oficina de 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 extralimiten sus funciones)									

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

ELABORÓ:	REVISÓ:	APROBÓ:
JOSE FERNANDO MORA MONTENEGRO Contratista / Oficina Asesora de Comunicaciones y Sistemas	LYDA ARGELIS PABON LOPEZ Jefe Oficina Asesora de Comunicaciones y Sistemas	DIEGO FERNANDO MORALES ORTEGÓN Gerente

8.3 FORTALECER LOS MECANISMOS DE RESPALDO DE LA INFORMACIÓN FÍSICA COMO DIGITAL PARA SU PRESERVACIÓN Y CONSERVACIÓN.

Permite garantizar el correcto funcionamiento del esquema de backups, de acuerdo al escenario de la arquitectura tecnológica, los cuales son necesarios para proteger y respaldar los activos de información y de esta manera garantizar fácilmente su recuperación en el momento de ser requerido.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT 900091143-9	PLAN DE ACCION DE AREAS, OFICINAS Y/O DEPENDENCIAS			
	VERSION	PROCESO/SERVICIO	CODIGO	NUM
	6.0	DIRECCIONAMIENTO ESTRATEGICO	DE-PAA	013

OFICINA ASESORA COMUNICACIONES Y SISTEMAS	VIGENCIA DEL PLAN DE ACCION	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	
Elaborar las copias de seguridad de las bases de datos de todo sistema de información integral de la empresa	Planificar la programación de backups de las bases de datos	1	Garantiza la disponibilidad, integridad y recuperación oportuna de la información crítica de la organización, minimizando el impacto de posibles pérdidas de datos y asegurando la continuidad operativa.	100%	No. de backups realizados automáticamente / No. de backups programados	Formato GSI-BDS-255	Enero 2025	Enero 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora Comunicaciones y Sistemas
	Ejecutar la programación de backups de las bases de datos	1		100%			Enero 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora Comunicaciones y Sistemas
	Evaluación continua y sistemática de los resultados de ejecución de las copias de respaldos (backups) para las bases de datos	1		100%		Informe	Diciembre 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora 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:
CHRISTIAN MUÑOZ DE LA ROSA Profesiona Universitario Oficina Asesora Comunicaciones y Sistemas	LYDA ARGELIS PABON LOPEZ Jefe Oficina Asesora Comunicaciones y Sistemas	DIEGO FERNANDO MORALES ORTEGÓN Gerente

8.4 GESTIONAR LOS INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A través de la detección y análisis de incidentes, se pueden identificar vulnerabilidades e implementar medidas correctivas para prevenir futuros eventos. Contamos con un procedimiento que permite manejar adecuadamente los incidentes de seguridad de la información.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT 900091143-9	PLAN DE ACCION DE AREAS, OFICINAS Y/O DEPENDENCIAS			
	VERSION	PROCESO/SERVICIO	CODIGO	NUM
	6,0	DIRECCIONAMIENTO ESTRATEGICO	DE-PAA	013

OFICINA ASESORA COMUNICACIONES Y SISTEMAS	VIGENCIA DEL PLAN DE ACCION	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	
Gestionar los Incidentes de Seguridad y Privacidad de la Información	Identificar recursos necesarios, definición de criterios de clasificación de los incidentes y definir los indicadores para evaluación y seguimiento.	1	Fortalecimiento de la capacidad de la organización para gestionar eficazmente los incidentes de seguridad de la información, garantizando una respuesta oportuna, la minimización de riesgos, el cumplimiento normativo y la mejora continua, lo que protege la confidencialidad, integridad y disponibilidad de la información crítica.	>=95%	Solicitud de gestión de incidentes de seguridad de la información resueltos	Procedimiento actualizado	Enero 2025	Enero 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora Comunicaciones y Sistemas
	Reporte de los incidentes de seguridad de la información a tarvés de la plataforma OsTickets	1				Reporte de incidentes Plataforma Osticket	Enero 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora Comunicaciones y Sistemas
	Seguimiento y evaluación a los indicadores de incidentes de seguridad de la información					Informe Mensual de Seguimiento y evaluación de indicadores de incidentes de seguridad de la información	Enero 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora Comunicaciones y Sistemas
	Realizar acciones de mejora	1				Acciones de Mejora	Diciembre 2025	Diciembre 2025	Jefe Oficina Asesora de Comunicaciones y Sistemas Profesional Universitario Oficina Asesora 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 ORTEGÓN Gerente

ANEXOS

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	RESOLUCIONES			
	VERSIÓN	PROCESO/SERVICIO	CODIGO	NUM
	6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-R	062
	GERENCIA			

RESOLUCIÓN No. 090
(27 de enero del 2025)

"Por la cual se adopta el Plan 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 publicalos 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 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 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 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 NIT.900091143-9	RESOLUCIONES			
	VERSIÓN	PROCESO/SERVICIO	CODIGO	NUM
	6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-R	062
	GERENCIA			

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 FERNANDO MORALES ORTEGÓN
Gerente.

Proyectó: WILLIAM RICARDO MONTENEGRO GUEVARA / Profesional Universitario

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 de 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

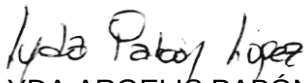
Fin del documento.

ACTUALIZADO POR:

WILLIAM RICARDO MONTENEGRO GUEVARA
Profesional Universitario
Oficina Asesora de Comunicaciones y Sistemas

JOSE FERNANDO MORA MONTENEGRO
Contratista Ingeniero de Sistemas
Oficina Asesora de Comunicaciones y Sistemas

REVISADO POR:



LYDA ARGELIS PABÓN LÓPEZ
Jefe
Oficina Asesora de Comunicaciones y Sistemas

APROBADO POR:

DIEGO FERNANDO MORALES ORTEGÓN
Gerente