



EMPRESA SOCIAL DEL ESTADO

**PASTO SALUD E.S.E**

NIT. 900091143-9

## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VERSIÓN 8.0

SAN JUAN DE PASTO  
2020

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	2

PASTO SALUD E.S.E.

ELABORO

WILLIAM MONTENEGRO GUEVARA  
JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

SAN JUAN DE PASTO  
2021

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	3

## TABLA DE CONTENIDO

### Contenido

INTRODUCCIÓN.....	6
1. OBJETIVO GENERAL.....	7
1.1. OBJETIVOS ESPECÍFICOS.....	7
2. ALCANCE.....	7
3. POLÍTICA DE SEGURIDAD DE LA INFORMACION.....	7
4. MARCO LEGAL.....	7
5. GLOSARIO.....	8
6. MODELO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN – SGSI.....	9
7. PERSONAL DE SEGURIDAD DE LA INFORMACION.....	10
8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.....	10
9. BIBLIOGRAFÍA.....	17

## ACTO ADMINISTRATIVO

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

**RESOLUCIÓN No.092**  
(29 de enero de 2020)

“Por la cual se adopta el Plan de Seguridad y Privacidad de la información de la Empresa Social del Estado Pasto Salud ESE”

La Gerente de la Empresa Social del Estado Pasto Salud E.S.E, en ejercicio de sus facultades legales y reglamentarias consagradas en la Ley 100 de 1.993, Decreto 1876 de 1.994, Acuerdo No.04 de 2006 emanado del Concejo Municipal de Pasto y Decreto No. 0530 del 30 de Septiembre del 2016 emanado por la Alcaldía Municipal de Pasto y,

**CONSIDERANDO:**

Que el Decreto 1078 de 2015, contempla en el artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la Información.

Que el Decreto 612 de 4 de abril de 2018, se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Que 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 el Plan de Seguridad y privacidad de la información se busca proteger la integridad y garantizar la disponibilidad y confidencialidad de todos los activos de información de la entidad.

Que mediante Resolución Interna No. 077 del 27 de Enero del 2020, se aprobó todos los Planes Operativos Anuales, dentro de la cuales se aprueba “Plan de Seguridad y Privacidad de la información” de la Empresa Social del Estado Pasto Salud E.S.E., la 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 E.S.E, documento que hace parte integral de la presente resolución.

**ARTÍCULO SEGUNDO.-** El Plan de Seguridad y Privacidad de la Información tiene como objetivo principal proteger la integridad y garantizar la disponibilidad y confidencialidad de la información de la Entidad.

**ARTÍCULO TERCERO.-** La actualización del documento adoptado mediante la presente Resolución, se realizará a través de acto administrativo de la misma categoría.

**ARTÍCULO CUARTO.-** Publíquese el presente acto administrativo en la página web de la Empresa Social del Estado Pasto Salud ESE.

**ARTÍCULO QUINTO.-** La presente resolución rige a partir de la fecha de su expedición.

**PUBLÍQUESE Y CÚMPLASE**

*Ana Belén Arteaga Torres*  
**ANA BELÉN ARTEAGA TORRES**  
Gerente

Proyectó: William Montenegro Guevara/ Jefe Oficina de Comunicaciones y Sistemas  
Revisó: José Luis Ocampo / Jefe Oficina Asesora Jurídica

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	5

### 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	
8.0	Actualización Plan de Seguridad y Privacidad de la Información.		X		<b>Justificación:</b> Se realiza ajuste a la política de Seguridad de la Información, Se ingreso 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
7.0	Elaboración del Documento Plan de Seguridad y Privacidad de la Información.	X			<b>Justificación</b> 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 092-29-01-2020

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	6

## INTRODUCCIÓN

La empresa Social del Estado Pasto Salud E.S.E, siguiendo las directrices en materia de seguridad digital y de la información de acuerdo, al Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital. Teniendo en cuenta lo anterior, se formula el Plan de Seguridad y privacidad de la información al interior de la Empresa Social del Estado Pasto Salud E.S.E.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	7

## 1. OBJETIVO GENERAL

Proteger los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

### 1.1. OBJETIVOS ESPECÍFICOS

- Identificar, clasificar, y gestionar los activos de la información de la empresa
- Apropiar al talento humano de la política de seguridad y privacidad de la información y su aplicación.
- Fortalecer los mecanismos de respaldo de la información física como digital para su preservación y conservación.

## 2. ALCANCE

Aplica a todas las sedes de Pasto Salud E.S.E, a todos sus grupos de interés 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 INFORMACION

La Empresa Social del Estado Pasto Salud E.S.E, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, administra, protege, preserva la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información en todos los procesos organizacionales, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

## 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.

**Ley 23 de 1982:** Sobre derechos de autor

**ISO IEC 27001-2013:** Estándares internacionales sobre tecnología de la información, técnicas de seguridad, Administración de seguridad de la información, los cuales proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de empresa.

**ISO IEC 27002-2013:** Es un estándar para la seguridad de la información.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	8

**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**, la cual se dictan disposiciones generales para la Protección de Datos Personales. Para conocer más de esta Ley

## 5. GLOSARIO

Entiéndanse para el presente documento los siguientes términos:

**Política:** Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización respecto a un asunto determinado.

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

**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.

**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.

**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.

**Criptografía de llave publica:** es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

**Cifrar:** quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama `descodificar" o `descifrar". Los sistemas de ciframiento se llaman `sistemas criptográficos".

**Certificado Digital:** es un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

**Controles sobre la seguridad:** representan los procedimientos de control interno establecidos por Pasto Salud E.S.E. para asegurar que el uso de las tecnologías de información alcance sus objetivos. En un concepto moderno y basado en los lineamientos que define la reingeniería organizacional, los controles generales se han direccionado al control de los procesos informáticos.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	9

**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.

**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.

**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.

**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.

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

**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.

**TI:** Tecnología de la Información.

**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.

**Spam:** Se llama spam, al correo basura o a los mensajes no solicitados, no deseados o de remitente desconocido.

**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.

**Sniffer:** El 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.

**Phishing:** El 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.

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



## 7. 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.

## 8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El plan de implementación para el componente de seguridad y privacidad de la información, comprende las siguientes actividades, cronograma y recursos asignados.

FORMULACIÓN PLAN OPERATIVO ANUAL

	VERSIÓN	PROCESO/SERVICIO	CÓDIGO	NÚM
	6.0	GESTION DE SISTEMAS DE INFORMACION	DE-POA	143

**ARTICULACIÓN PLAN DE DESARROLLO INSTITUCIONAL OBJETIVO ESTRATÉGICO 2021 - 2024**

Mejorar continuamente los procesos de direccionamiento, gerencia, atención al cliente asistencial y de apoyo administrativo, mediante la implementación de procesos de mejoramiento de la calidad y asumiendo los resultados de autoevaluaciones periódicas.

OBJETIVO ESPECÍFICO 1		INDICADOR	META	EVIDENCIAS	PLAZOS		RESPONSABLES		PRESUPUESTO (INVERSIÓN)			EVIDENCIA APORTADA	
					INC	FIN	LÍDER	EQUIPO	APLICA		MONTO		
ACTIVIDADES		PHVA							SI	NO			
1	Identificar, clasificar, y gestionar los activos de la información de la empresa	PHVA	Activos de la información, Esquema de Publicación e índice de clasificación actualizados	>=90%	Publicación en la página web	Marzo	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		X	Hosting Valor=\$2.994.070 Cloud Backup Valor= \$32.548.079	
1.1	Establecer el instrumento, la metodología para el levantamiento de activos de la información y el mecanismo de respaldo.	PLANEAR	NA	100%	. Acta de reunión para levantamiento de activos de la información. . Programación de respaldo de los activos de la información	Febrero	Marzo	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		

1.2	Socializar la metodología, el instrumento para la recolección, consolidación y clasificación de los activos de Información, así como el mecanismo de respaldo.	HACER	No de personas a quien se socializó la guía/Total de Personas programadas para la socialización	>=90%	Invitación con Circular a la socialización Reuniones Virtuales y registro de asistencia	Marzo	Marzo	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		
1.3	Consolidar, actualizar y publicar los activos de la información.	HACER	No de activos de la información identificados, clasificados y publicados	100%	Publicación del documento de los activos de la información en la página web.	Abril	Abril	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		
1.4	Realización de auditoria de seguridad de la información.	HACER	NA	100%	Informe de auditoría al seguimiento de aplicación de políticas de seguridad informática y de la información en las IPS auditadas.	Mayo	Octubre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Oficina de Comunicaciones y Sistemas		X		
1.5	Evaluar los resultados obtenidos de la auditoria de seguridad de la información.	VERIFICAR	Numero de No cumplimiento s a la política de seguridad de la información/ Total de ítems de seguridad de la información aplicados	100%	Informe de Auditoría	Junio	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		

1.6	Identificación de oportunidades de mejora frente a resultados no esperados	ACTUAR	No de oportunidades de mejora cumplidas/Total de mejoras identificadas	100%	Análisis de Causa Plan de mejora	Junio	Junio	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		
<b>OBJETIVO ESPECIFICO 2</b>													
2	Apropiar al talento humano de la política de seguridad y privacidad de la información y su aplicación		No de capacitaciones realizadas/Total de programación programadas	>=90%	Registro de capacitaciones Plataforma aula Virtual, Evaluaciones realizadas	Junio	Noviembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		x		
<b>ACTIVIDADES</b>		<b>PHVA</b>											
2.1	Planificar las temáticas de capacitación de seguridad de la información en el Plan Institucional de Capacitaciones PIC	PLANEAR	NA	100%	Plan Institucional de capacitaciones PIC	Enero	Enero	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		
2.2	Planificar la auditoria de seguridad de la Información	PLANEAR	NA	100%	Acta de la planificación y Oficio enviado de la programación a las Direcciones operativas de red	Abril	Octubre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		
2.3	Ejecutar el plan de capacitaciones de seguridad de la información	HACER	No de personas capacitadas/ Total de personas programadas	>=90%	Piezas Gráficas Plataforma moodel Página Seguridad de la Información Reunión Virtual Registro	Mayo	Noviembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		

					asistencia a Capacitación							
2.4	Realización de auditoria de seguridad de la información.	HACER	NA	100%	Informe de auditoría al seguimiento de aplicación de políticas de seguridad informática y de la información en las IPS auditadas.	Mayo	Octubre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Oficina de Comunicaciones y Sistemas		X	
	Evaluar los resultados obtenidos de la auditoria de seguridad de la información.	VERIFICAR	Numero de No cumplimiento s a la política de seguridad de la información/ Total de ítems de seguridad de la información aplicados	100%	Informe de Auditoría	Junio	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x	
2.5	Socializar la política de seguridad de la información y Promover el uso de mejores prácticas de seguridad de la información, para minimizar riesgos.	HACER	Número de fallas o no cumplimiento s encontrados en las sensibilizaciones programadas o eventos	<b>Mínima</b> : >=75% y <80% <b>Satisfactoria</b> : >=80% y <90% <b>Sobresaliente</b> :	Informe Semestral de evaluación	Junio	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Oficina de Comunicaciones y Sistemas		x	

			realizados para evaluar el tema/ Total de personas a capacitar.	>=90%								
2.6	Identificación de oportunidades de mejora frente a resultados no esperados	ACTUAR	No de oportunidades de mejora cumplidas/Total de mejoras identificadas	100%	Análisis de Causa Plan de mejora	Junio	Junio	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x	
<b>OBJETIVO ESPECÍFICO 3</b>												
3	Fortalecer los mecanismos de respaldo de la información física como digital para asegurar su preservación y conservación		No de Backups realizados / No de Backups programados	>=99%	Bitácora de Jobs SQL Server de backup realizados exitosamente . Bitácora de realización de Informe de Backups mensual GSI-BDS 255	Enero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		x	Cloud Backup Valor= \$32.548.079
<b>ACTIVIDADES</b>		<b>PHVA</b>										
3.1	Planificación de la programación de Backups de las bases de datos	PLANEAR	NA	100%	Acta de levantamiento de bases de datos para realizar la programación de los backups.	Febrero	Febrero	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		x	

3.2	Ejecución del programa de backups para las bases de datos	HACER	NA	100%	'Bitácora de Jobs SQL Server de la programación de backups y la ejecución.	Enero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		x		
3.3	Evaluación continua y sistemática de los resultados de ejecución de las copias de respaldo(backups) para las bases de datos		No de Backups realizados / No de Backups programados	>=99%	Bitácora de realización de Informe de Backups mensual GSI-BDS 255	Enero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		x		
3.4	Identificación de oportunidades de mejora frente a resultados no esperados	ACTUAR	No de oportunidades de mejora cumplidas/Total de mejoras identificadas	100%	Análisis de Causa Plan de mejora	Junio	Junio	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x		

 <b>EMPRESA SOCIAL DEL ESTADO</b> <b>PASTO SALUD E.S.E</b> <small>NIT. 900091143-9</small>	PLAN EMPRESARIAL DE EMERGENCIAS			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Secretaría General	PL- EM	6.0	17

## 9. 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

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	6.0	18

Fin del documento.  
ELABORADO POR:

EQUIPOS OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

REVISADO POR:

WILLIAM MONTENEGRO GUEVARA  
JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

APROBADO POR:

ANA BELÉN ARTEAGA TORRES  
Gerente