

ESTADO
E.S.E
981143-9

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

FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
Secretaría General	PL- EM	9.0	1



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 9.0

SAN JUAN DE PASTO
2022


	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	2

TABLA DE CONTENIDO

INTRODUCCIÓN	6
1	7
1.1.	7
2	7
3	7
4	7
5	7
6	9
7	10
7.1	10
7.1.1	10
7.1.2	10
8	11
9	14
10	21
11	21
12	21
13	26



FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	3

ACTO ADMINISTRATIVO

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	RESOLUCIONES			
	VERSIÓN	PROCESO/SERVICIO	CÓDIGO	NUM
	6.0	GESTIÓN DE SISTEMAS DE INFORMACIÓN	GSIR	062
	GERENCIA			

RESOLUCIÓN No. **076**
(25 de enero de 2022)

"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 2022"

LA GERENTE (E)

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 Decreto 224 del 30 de abril de 2020 y Resolución 006 de 13 de Enero del 2022 expedidas por Alcaldía Municipal de Pasto 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 publicarlos 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 001-2022 del Comité Institucional de Gestión y Desempeño del día 25 de enero de 2022 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 2022, 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 2022", 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 gestionar los 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.

ARTÍCULO TERCERO. - Publíquese el presente acto administrativo en la página web de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2022".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	4

	RESOLUCIONES			
	VERSIÓN	PROCESO/SERVICIO	CODIGO	NUM
	9.0	GESTION DE SISTEMAS DE INFORMACION	CS-R	052


GERENCIA

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

PUBLÍQUESE Y CÚMPLASE


 ADRIANA DEL ROCÍO ENRIQUEZ MEZA
 Gerente (E)


Proyecto: Harvey Alexis Vallejo Narváez / Jefe Oficina de Comunicaciones y Sistemas
 Revisó: José Luis Ocampo / Jefe Oficina Asesora Jurídica

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	5

CONTROL DE CAMBIOS

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


Versión	CONTROL DE CAMBIOS	INFORMACIÓN DE CAMBIOS			Acto Administrativo de Adopción		
		E	M	X			
9.0	Actualización Plan de Seguridad y Privacidad de la Información		X		Justificación: Se incluye la matriz actualización de la matriz de riesgos Se realiza ajuste a las Actividades de la poa vigencia 2022	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Profesional Universitario	Resolución 076-01-2022
8.0	Actualización Plan de Seguridad y Privacidad de la Información		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 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 093-29-01-2020

 EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E <small>NIT. 900091143-9</small>	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	6

INTRODUCCIÓN

Hoy en día, las empresas, reconocen que la información es el principal activo en sus procesos, por tanto, la importancia de tener su información adecuadamente identificada y protegida, es quizá el mayor reto que se tiene para dar cumplimiento a un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia. La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad.

El plan de tratamiento de riesgos tiene un propósito preventivo a través de la planeación e implementación de acciones y medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre reducir la afectación a la entidad en caso de materialización.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	7

1 OBJETIVO GENERAL

Controlar y minimizar los riesgos asociados a la seguridad y privacidad de la información con el fin de reducir la probabilidad y el impacto adverso de los incidentes y salvaguardar los activos de información existentes, en la Empresa Social de Estado Pasto Salud.

1.1. OBJETIVOS ESPECÍFICOS

- Identificar, analizar y evaluar los riesgos de Seguridad de la información
- Gestionar los incidentes de Seguridad y Privacidad de la Información para mitigar el riesgo de forma efectiva, eficaz y eficiente

2 ALCANCE

Aplica a todas los procesos y sistemas de información de la empresa social del estado Pasto salud E.S.E. teniendo en cuenta los riesgos altos y extremos.

3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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.


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.

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).

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	8

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 que 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

PROCESO PARA LA ADMINISTRACIÓN DEL RIESGO.



	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	10

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
Pérdida 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

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	11

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	<ul style="list-style-type: none"> • Piratería • Ingeniería Social Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Dstrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	<ul style="list-style-type: none"> • Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Dstrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	<ul style="list-style-type: none"> • Bomba/Terrorismo • Penetración en el sistema • Manipulación en el sistema
Espionaje	Ventaja competitiva Espionaje económico	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación) 	<ul style="list-style-type: none"> • 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.
SOFTWARE	Copia no controlada	Hurtos medios o documentos.
	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 autenticación, como la autenticación 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
	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 auditorías	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
	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

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	14

9 IDENTIFICACIÓN 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 continuas.
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.
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.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	15


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.
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 crítica, 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 pérdida, 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.
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 pérdida 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 auditorías 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.

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
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.


	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	18

A.17.1.2	<i>Implementación de la continuidad de la seguridad de la información</i>	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

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Secretaría General	PL- EM	9.0	19

10 IDENTIFICACIÓN DE RIESGOS DE LA INFORMACIÓN PARA PASTO SALUD ESE

No	RIESGOS	VALORACIÓN SEVERIDAD DEL RIESGO ANTES DE CONTROLES			VALORACIÓN SEVERIDAD DEL RIESGO DESPUÉS DE CONTROLES				PRIORIZACIÓN
		Probabilidad de Ocurrencia (inherente)	Impacto Inherente	NIVEL	No de controles aplicado	Probabilidad con controles	Impacto con controles	NIVEL	
R1	Posibilidad de perder completitud, exactitud y 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.	80%	80%	ALTO	4	7%	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.	100%	80%	ALTO	5	8%	80%	ALTO	SI
R3	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.	100%	100%	EXTREMO	5	13%	65%	MODERADO	SI
R4	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	100%	80%	ALTO	3	22%	80%	ALTO	SI

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	20

	parte del proveedor, ausencia de equipos para la protección externa y conexiones de red sin protección.								
R5	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.	80%	80%	ALTO	6	4	52	MODERADO	SI
R6	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 los tiempos de entrega y recepción de documentos.	80%	80%	ALTO	2	29%	80%	ALTO	SI

11 TRATAMIENTO DE RIESGOS

Ver: Matriz de Tratamiento de Riesgos

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Secretaría General	PL- EM	9.0	21

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



13 PERSONAL DE SEGURIDAD DE LA INFORMACIÓN

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 TRATAMIENTO DE RIESGOS

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

FORMULACIÓN PLAN OPERATIVO ANUAL			
VERSIÓN	PROCESO/SERVICIO	CÓDIGO	NÚM
6.0	GESTIÓN DE SISTEMAS DE INFORMACION	DE-POA	143

ARTICULACIÓN PLAN DE DESARROLLO INSTITUCIONAL OBJETIVO ESTRATÉGICO 2021 - 2024	Mejorar continuamente los procesos de dirección, 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)				
					IN	FI	LÍDER	EQUIPO	APLICA		MONTO	EVIDENCIA APORTADA	
ACTIVIDADES		PHVA							SI	NO			
1	Identificar, analizar y evaluar los riesgos de seguridad de la información	Matriz de Riesgos	>=90%	Plan de Tratamiento de Riesgos	Febrero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas	X			Antivirus Valor: \$27.361.950 Seguridad Perimetral Valor: \$54,451,211	
1.1	Revisión y actualización de la matriz de riesgos	PLAN EAR	NA	100%	Actualización de la matriz de identificación, análisis y evaluación de riesgos	Febrero	Febrero	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		X		



1.2	Socialización de la matriz de riesgos y Plan de tratamiento de Riesgos al equipo de la Oficina de Comunicaciones y Sistemas	HACER	No de personas a quien se socializa la temática/Total de Personas programadas para la socialización	100%	Correo electrónico Reuniones Virtuales y registro de asistencia	Marzo	Marzo	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas		x	
1.3	Evaluación de la efectividad de los controles	VERIFICAR	Efectividad de la Probabilidad: Calificación Total de controles que reducen la probabilidad/ No. De Controles que reducen la probabilidad Efectividad del Impacto: Calificación Total de controles que reducen el impacto/ No. De Controles que reducen el impacto	>=90%	Informe de seguimiento al cumplimiento de tratamiento de riesgos.	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	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Comunicaciones y Sistemas Archivo y Correspondencia		x	




OBJETIVO ESPECÍFICO 2															
2	Gestionar los incidentes de Seguridad y Privacidad de la Información para mitigar el riesgo de forma efectiva, eficaz y eficiente	Total, de Incidentes gestionados y cerrados/Total Incidentes Notificados	100%	Informe plataforma Ostickets Tema Incidentes de Seguridad de la Información	Febrero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Profesional Universitario Seguridad de la Información	X					Hosting Valor=\$ 3,143,774	
ACTIVIDADES		PHVA													
2.1	Clasificación y priorización de los incidentes de seguridad de la información.	PLANEAR	NA	100%	Acta equipo de seguridad de la información	Febrero	Febrero	Jefe Oficina Asesora de Comunicaciones y Sistemas	Profesional Universitario Seguridad de la Información		X				
2.2	Socializar el procedimiento de incidentes de seguridad de la información con el personal técnico en sistemas de Pasto Salud.	HACER	No de personas a quien se socializó la temática/Total de Personas programadas para la socialización.	100%	Invitación por correo electrónico para la socialización. Reunión Virtual y registro de asistencia	Febrero	Febrero	Jefe Oficina Asesora de Comunicaciones y Sistemas	Profesional Universitario Seguridad de la Información		X				
2.3	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento.	HACER	Total, de Incidentes gestionados y cerrados/Total Incidentes Notificados	100%	Plataforma Ostickets Informe Trimestral de Gestión de Tickets	Febrero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Profesional Universitario Seguridad de la Información		X				

2.4	Evaluación del impacto de los incidentes de seguridad de la información	VERIFICAR	No de incidentes que tienen un alto impacto en la seguridad de la información/Total de incidentes de seguridad de la información reportados	100%	Informe Trimestral de seguimiento y análisis de incidentes	Febrero	Diciembre	Jefe Oficina Asesora de Comunicaciones y Sistemas	Profesional Universitario Seguridad de la Información		X			
2.5	Identificación de oportunidades de mejora referente a incidentes de información	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			

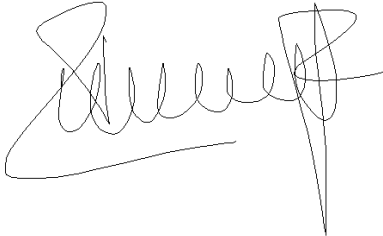
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Secretaría General	PL- EM	9.0	26

15 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 TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	FORMULACIÓN	CÓDIGO	VERSIÓN	PÁG.
	Oficina Asesora de Comunicaciones y Sistemas	MA- PSII	9.0	27

Fin del documento.
ELABORADO POR:



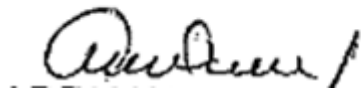
WILLIAM RICARDO MONTENEGRO GUEVARA
PROFESIONAL UNIVERSITARIO

REVISADO POR:



HARVEY ALEXIS VALLEJO NARVAEZ
JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

APROBADO POR:



ADRIANA ENRIQUEZ MEZA
Gerente (E)