EMPRESA SOCIAL DEL ESTADO

PASTO SALUD E.S.E

NIT.900091143-9

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

VERSIÓN 6.0

SAN JUAN DE PASTO
2020

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

ELABORO

WILLIAM MONTENEGRO GUEVARA
JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

SAN JUAN DE PASTO
2020

TABLA DE CONTENIDO

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

RESOLUCIÓN No. 093
(29 de enero de 2020)

"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"

LA 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 dela 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 612 del 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 Resolución Interna No.077 del 27 de Enero de 2020, se aprobó Plan Estratégico de las Tecnologías de la Información de la Empresa Social del Estado Pasto Salud ESE, la cual se pretende adoptar mediante el presente acto administrativo.

En mérito de lo expuesto,

RESUELVE:

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

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

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

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E	RESOLUCIONES			
	VERSIÓN	PROCESO/SERVICIO	CODIGO	NUM
	6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-R	082
	OFICINA DE COMUNICACIONES Y SISTEMAS			

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

Firma en Original
ANA BELÉN ARTEAGA TORRES
Gerente.

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

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	
6.0	Elaboración del Plan de Tratamiento de Riesgos 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 del 29 de enero de 2020

INTRODUCCIÓN

Hoy día, las empresas reconocen el protagonismo de la información en sus diferentes procesos, por tanto es una prioridad que la información esté adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, de esta manera se requiere dar 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 ante una serie de amenazas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, es a través de la implementación de medidas de control de seguridad de la información, lo que permitirá gestionar y reducir los riesgos e impactos a que está expuesta.

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. Decide entonces vincular el modelo de tratamiento de los riesgos de seguridad y privacidad de la información en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

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.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar los riegos, Amenazas y vulnerabilidades de seguridad y privacidad de la información
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.
- Proteger el valor de los activos de información mediante la implementación de controles para mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente

1.3 ALCANCE

La gestión y el tratamiento de riesgos de seguridad y privacidad de la información, podrá será aplicada sobre cualquier proceso de la empresa, a cualquier sistema de información, Infraestructura informática o aspecto particular de control de la Entidad, a través de la metodología establecida para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formatos que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye implementación de controles, recomendaciones para su seguimiento, monitoreo y evaluación.

2. 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.

3. 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.

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

4. GLOSARIO

Entiéndanse para el presente documento los siguientes términos:

Política: Son instrucciones mandatorios 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.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

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

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

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

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

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

PROCESO PARA LA ADMINISTRACIÓN DEL RIESGO

6. IDENTIFICACIÓN DE AMENAZAS

D: Deliberadas **A:** Accidentales **E:** Ambientales

Amenazas Comunes

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

Amenazas Humanas

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Penetración en el sistema • Manipulación en el sistema
Espionaje	Ventaja competitiva Espionaje económico	• Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes y despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación	• Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

7. IDENTIFICACIÓN DE VULNERABILIDADES

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

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Error en el uso
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Error en la disposición final de los medios
	Ausencias de pistas de auditoria	Error en el software
	Asignación errada de los derechos de acceso	Error en la asignación de perfiles
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas	Espionaje remoto

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
RED	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Daño de equipos y medios
	Inducción insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
PERSONAL	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Abuso de los derechos
	Ubicación en área susceptible de inundación	Abuso de los derechos
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
ORGANIZACIÓN	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en la prestación de los servicios
	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	Error en el uso

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
	descripción de los cargos	
	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

8. IDENTIFICACIONES DE CONTROLES

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

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
A.9.1	Requisitos de la organización para control de acceso	**Objetivo**: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	**Control**: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos de la organización y de seguridad de la información
A.9.1.2	Política sobre el uso de los servicios de red	**Control:** Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios	**Objetivo**: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios	**Control**: Se debe implementar un protocolo formal para el registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control**: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.6	Retiro o ajuste de los derechos de acceso	**Control**: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las Instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios
A.9.4.1	Restricción de acceso Información	**Control**: El acceso a la información y a las funciones de los sistemas de las aplicaciones se deben restringir de acuerdo con la política de control de acceso
A.9.4.3	Sistema de gestión de contraseñas	**Control**: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones
A.9.4.5	Control de acceso a códigos fuente de programas	**Control**: Se debe restringir el acceso a los códigos fuente de los programas.
A.10.1	Controles criptográficos	**Objetivo**: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos	**Control**: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.11.1	Áreas seguras	**Objetivo**: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización
A.11.1 1	Perímetro de seguridad física	**Control**: Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información
A.11.1 2	Controles físicos de entrada	**Control**: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado
A.11.1 4	Protección contra amenazas externas y ambientales	**Control**: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.2	Equipos	**Objetivo**: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
		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 negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
A.12.2	Protección contra códigos maliciosos	**Objetivo**: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	**Control**: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo	**Objetivo**: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información	**Control**: Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada
A.12.4	Registro y seguimiento	**Objetivo**: Registrar eventos y generar evidencia.
A.12.4.4	sincronización de relojes	**Control**: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo
A.12.5	Control de software	**Objetivo**: Asegurar la integridad de los sistemas

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
	operacional	operacionales.
A.12.5.1	Instalación de software en sistemas operativos	**Control**: Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos
A.12.6	Gestión de la vulnerabilidad técnica	**Objetivo**: Prevenir el aprovechamiento de las vulnerabilidades técnicas
A.12.6.2	Restricciones sobre la instalación de software	**Control**: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales
A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio
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 del negocio 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

No	NOMBRE	DESCRIPCIÓN/JUSTIFICACIÓN
		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 negocio de la organización
A.17.1.1	*Planificación de la continuidad de la seguridad de la información*	**Control**: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	*Implementación de la continuidad de la seguridad de la información*	*Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.*
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Control**: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas
A.18.1	Cumplimiento de requisitos legales y contractuales	**Objetivo**: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.2	Derechos de propiedad intelectua	**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

9. MATRIZ DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	MATRIZ DE RIESGOS (PARTE B)		
VERSIÓN	PROCESO / SERVICIO	CÓDIGO	NÚM.
6.0	GESTIÓN DE CONTROL	GC-MR	079

FECHA DE ACTUALIZACIÓN:	13 de diciembre de 2018	MACROPROCESO	GESTIÓN DE SISTEMAS DE INFORMACION

PROCESO	RIESGO (Que evento puede suceder)	AGENTE GENERADOR	ANÁLISIS DE CAUSAS (Debido a)	EFECTOS O CONSECUENCIAS (Potenciales)	VALORACIÓN DEL RIESGO SIN CONTROLES			CONTROLES	VALORACIÓN DEL RIESGO DESPUÉS DE CONTROLES			TRATAMIENTO					
					PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACIÓN		MEDIO DE EVIDENCIA
															INICIO	FINAL	
1	Destrucción y/o pérdida de los activos de información (Físicos, Digitales y Electrónicos)	Medioambiente. Social. Personas. Infraestructura.	• Debido a Erupción Volcánica. • Debido a terremoto. • Debido a Incendios. • Debido a Inundaciones. • Debido a actos terroristas. • Debido a actos mal intencionado por empleados o personas externas. • Debido al uso	• Sanciones disciplinarias, penales y fiscales. • Interrupción del servicio. • Pérdidas económicas. • Insatisfac	MODERADA	CATASTRÓFICA	**EXTREMO**	Política de copias de seguridad de la información de todas las bases de datos y la información de los equipos priorizados y críticos que	RARA	MODERADA	**MODERADO**	**EVITAR**	1. Contratar el servicio de respaldo de la información en la nube para la vigencia.	Jefe Oficina Asesora de Comunicaciones y sistemas	01/01/2020	15/01/2020	Contrato del servicio

			inadecuado o mal uso de los equipos y redes de datos por parte de los funcionarios y contratistas de la Empresa. • Debido a sitios o espacios que no cumplen con las condiciones adecuadas para el almacenamiento de los medios que guardan la información de la Empresa. • Debido a fallas técnicas en hardware, software, red de datos, equipos de telecomunicaciones y redes eléctricas. . Debido a la Ausencia de Protección en Hardware • Debido a ausencia de protección en el control documental . Debido al desconocimiento o incumplimiento de la política y buenas prácticas de seguridad y privacidad de la información.	ción del usuario final. • Mala imagen institucional				contienen información relevante para la institución. (Programación automática en la nube).							
								Políticas de restricción de accesos a nivel de software, hardware y red de datos mediante perfiles de usuario y claves de acceso.				2. Mantenere implementar políticas para: Acceso a la red de datos, contraseñas de directorio activo. . Cambio de contraseñas. . Restricción de dispositivos móviles. . Restricción de dispositivos USB. . Restricción de tiempos de trabajo en los equipos . Crear	Comité de Contratación Jefe Oficina Asesora de Comunicaciones y sistemas	01/02/2020	30/04/2020	Políticas implementadas en el directorio activo

												Grupos de usuarios y nuevos perfiles de administradores . Implementar política de restricción y uso de aplicaciones. . Restricción de Panel de control del sistema Operativo. . Restricción para a instalación de software.				
								Políticas de seguridad perimetral				3 Implementación de políticas de acceso en el firewall fortinet	Profesional Universitario Sistemas	01/02/2019	31/04/2019	Políticas implementadas en la UTM Fortinet
								Implementación de UPS y plan de mantenimiento de la red eléctrica				4. Compra de Ups de acuerdo al plan de compras y priorización de las IPS Realizar mantenimiento	Contratista Supervisor del Contrato	01/02/2020	30/11/2020	Ups adquiridas, contrato de mantenimiento y cronograma del plan de manteni

												preventivo y correctivo a las UPS				miento hospitalario
								Auditoría para verificar el cumplimiento de la política y buenas prácticas de seguridad y privacidad de la información.				5. Realización de la auditoria interna de seguridad de la información a las IPS priorizadas según el POA de seguridad y privacidad de la información.	Ingeniero de Sistemas	01/05/2020	30/09/2020	Informe de auditoría y planes de mejora
								Política de control de edición e impresión de documentos institucionales almacenados en el servidor documental.				6. Aplicar mediante la herramienta adobe el control de edición e impresión a los documentos almacenados en el servidor documental y	Ingeniero de Sistemas y Profesionales Universitarios Planeación	01/01/2020	31/12/2020	Documentos protegidos en servidor documental y publicados

													publicado.				
								Políticas de seguridad a nivel de hardware y software en el antivirus					7. Restricción de aplicaciones y dispositivos.	Profesional Universitario Sistemas	01/02/2019	31/12/2020	Políticas implementadas en plataforma antivirus.
								Política de control de acceso físico a través de clave y bitácora de registro al Data Center donde se encuentran los servidores y equipos de comunicaciones.					8. Cambio de clave de acceso al Data Center. Llevar el registro de la bitácora de ingreso al data center. Instalación cámara de seguridad al interior del data center.	Ingeniero, Profesional de Sistemas, Jefe Oficina Asesora de Comunicaciones y sistemas	01/02/2020	31/12/2020	Cámara de seguridad instalada. Clave asignada a la data center y bitácoras de registro de ingreso y salida.
2	Inoportunidad en el reporte y entrega de informes a Entidades	Personas.Tecnología.Proceso	Debido al desconocimiento de la norma aplicable.Debido a la rotación de personal.Debido a fallas tecnológicas.Debido a la demora en la entrega de información entre Dependencias.	Sanciones	MODERADA	MAYOR	EXTREMO	Revisión de la matriz plan general de informes	RARA	MAYOR	ALTO	EVITAR	1. Envió de correo a los responsables de entrega de información de la matriz general de	Jefe Oficina Asesora de Comunicaciones y Sistemas.	01/02/2020	29/02/2020	Comunicación correo electrónico

													informes.				
								Actualización de la matriz del plan general de informes.					2. Eliminar informes obsoletos e ingresar en la matriz nuevos informes	Jefe Oficina Asesora de Comunicaciones y Sistemas y Profesionales Oficina Asesora de Planeación	01/03/2020	31/12/2020	Publicación Pagina web
								Publicación de la matriz plan general de informes					3. Matriz plan general de informes publicado en página web y Seguimiento al Plan general de informes.	Profesional Universitario Sistemas y Oficina de Control interno	01/03/2020	31/12/2020	Lista de chequeo a seguimiento de la matriz
3	Perdida de integridad de los datos registrados en los registros clínicos.	Personas. Tecnología.	Debido a errores intencionales y no intencionales por parte del responsable. Debido a la falta de validación de la información del Sistema SIOS. Debido a hardware	Inadecuada toma de decisiones. Sanciones. Afectación de la credibilidad e	PROBABLE	MAYOR	EXTREMO	Capacitación al personal en guías y protocolos de atención	IMPROBABLE	MENOR	BAJO	EVITAR					

			y software obsoleto.	imagen Institucional.				Validación en los registros clínicos a nivel de software								
								Seguimiento y validación de la información de los registros clínicos								
								Reporte de errores de inconsistencia encontrados en los registros clínicos								
4	Deterioro de los documentos	Infraestructura Recursos	• No contar con una infraestructura adecuada para la custodia de documentos. • De forma natural y de forma accidental • Ausencia de equipos de control del ambiente y de prevención de incendios • Ausencia de elementos necesarios para la protección y preservación de los documentos.	• Sanciones disciplinarias, penales y fiscales. • Pérdida de memoria y de información del proceso. • Ilegibilidad de los soportes probatorios. • Perdida de Imagen de la entidad	PROBABLE	MAYOR	EXTREMO	Digitalización y almacenamiento de los documentos.	PROBABLE	MAYOR	EXTREMO	EVITAR	1. Socialización al personal de gestión de archivo la manera de digitalizar documentos para su almacenamiento.	Oficina Asesora de Comunicaciones y Sistemas y Oficina de Archivo y Correspondencia	01/03/2020	30/03/2020	Firma de personas convocadas a la socialización
													2. Implementación del sistema de gestión documental	Oficina Asesora de Comunicaciones y Sistemas y Oficina de Archivo y Correspondencia	01/03/2020	30/07/2020	Sistema de Gestión documental implementado

	Documentos no Controlados	Personas	Falta de Herramientas tecnológicas para garantizar Seguridad en Documentos No seguir los lineamientos del protocolo de estandarización documental y el procedimiento. Falta mayor control de la documentación en las sedes Falta capacitación al personal en el uso y control de los documentos. Falta de conocimiento de la normatividad que	• Sanciones disciplinarias, penales y fiscales. • No conformidades en la prestación del servicio • Reprocesos en el diligenciamiento de los formatos de registros. • Mala toma de				1. Adquisición de Herramienta Adobe Suite para control documental en formato puf contra impresión, modificación.								
								2. Seguimiento para el control de la información documentada.								

5			rige el control documental.	decisiones por mal uso de los documentos.				3. Protocolo de control de la información documentada									
6	Desinformación o ruido mediático	Personas. Medios de Comunicación	Debido a información inoportuna y no confiable. Debido al desconocimiento de los protocolos establecidos	Afectación de la imagen, credibilidad y confianza en la gestión asistencial y administrativa de las partes interesadas pertinentes.	PROBABLE	MODERADA	ALTO	Conformación del Comité Editorial	IMPROBABLE	MODERADA	MODERADO	ASUMIR					
								Capacitación al personal en el protocolo de relaciones públicas y comunicación de crisis.									
7	Inadecuada comunicación y transmisión de la información	Personas. Recursos.	Debido a una mala planeación de las estrategias comunicacionales.	Distorsión de la información recibida	MODERADA	MENOR	MODERADO	Planear las estrategias comunicacionales	IMPROBABLE	MENOR	BAJO	ASUMIR					

			Debido a la desarticulación con los procesos o dependencias generadoras de información. Debido a la aplicación de una metodología inadecuada de diseño.	por las partes interesadas				Recolectar información de los procesos organizacionales para el diseño de las estrategias comunicacionales.								
								Identificar las herramientas tecnológicas para el diseño apropiado de cada estrategia comunicacional								

ELABORO	REVISO	APROBÓ (Líder de Proceso)

BIBLIOGRAFÍA

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Resolución 2999 del 2008.** Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- **Resolución 2007 de 2018.** Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital

Fin del documento.

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