HOSPITAL CIVIL DE IPIALES
EMPRESA SOCIAL DEL ESTADO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CODIGO: MP - 0444
VERSION: 4
VIGENCIA: 31/01/2025
REVISIÓN: 31/01/2025

ELABORÓ	REVISÓ	APROBÓ
ROBINSON PROAÑO QUISTIAL LIDER GERENCIA DE LA INFORMACION	GABRIELA CHAMORRO HUERTAS P.U GESTION DE CALIDAD	JESSIKA BONILLA SANTIUSTY EN PLANEACION
FECHA 31 – ENERO - 2025	**FECHA** 31 – ENERO - 2025	**FECHA** 31 – ENERO - 2025

2025

Contenido

1. INTRODUCCIÓN

Este documento busca lograr la implementación en el Hospital Civil de Ipiales E.S.E de las mejoras prácticas planteadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información, en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información.

El Modelo de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

2. OBJETIVOS

OBJETIVO GENERAL

Establecer las políticas, prácticas y lineamientos que permitan a la organización garantizar la adecuada protección de todos sus activos de información y prevenir la materialización de riesgos que puedan afectar su confidencialidad, integridad y disponibilidad de la información.

OBJETIVO ESPECIFICO

1. Gestionar oportunamente el riesgo en el manejo de la información de los procesos misionales de la entidad.

2. Cumplir con los principios de seguridad de la información en la confidencialidad, integridad y disponibilidad.

3. Cumplir con los principios de la función pública.

4. Mantener la confianza de los funcionarios, contratistas y terceros sobre la protección de su información.

5. Apoyar la innovación tecnológica que contribuya a la protección de la información y datos personales

6. las políticas, procesos, lineamientos, procedimientos en materia de seguridad de la información para la protección de la información y datos personales.

7. Fomentar una cultura de seguridad de la información en los colaboradores de la organización.

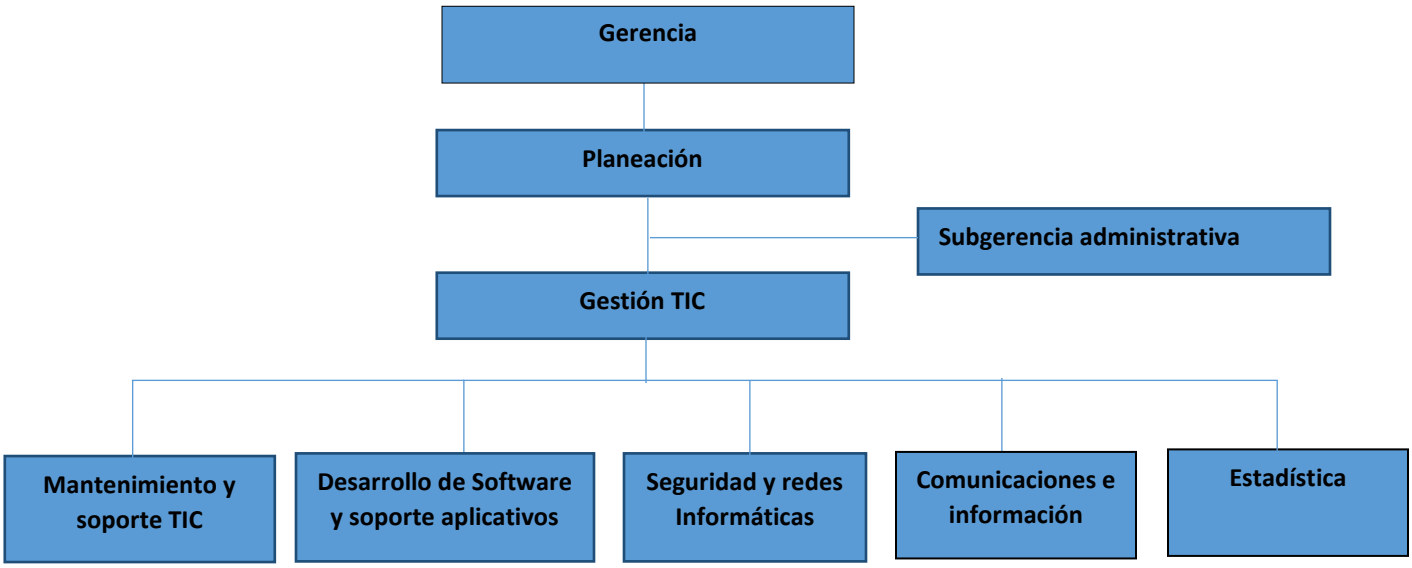
8. Garantizar la continuidad de la seguridad de la información frente a eventos adversos.

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica para todos los colaboradores, incluyendo los proveedores de servicios externos, contratistas y demás grupos de valor del HOSPITAL CIVIL DE IPIALES E.S.E.

4. RESPONSABLES

La estructura organizacional del proceso de Gestión TIC del Hospital civil de Ipiales es de la siguiente manera:



- Gerente
- Jefe de planeación
- Subgerente Administrativo
- Líder del proceso de Gestión Tic
- Profesional del área de estadística
- Profesional del área de comunicaciones
- Profesionales y técnicos en mantenimiento de computadores
- Auxiliares en mantenimiento de computadores
- Ingenieros de desarrollo de software.
- Auxiliar administrativo.

Política de gerencia de la información

El equipo de colaboradores y el Gerente del Hospital Civil de Ipiales E.S.E., se comprometen a generar información oportuna, clara, segura y confiable a sus usuarios y su familia, clientes internos y externos garantizando la transparencia y el acceso a la información pública, apoyados el cumplimiento de los principios orientadores de organización de las Técnicas de Información y Comunicación (TIC), con énfasis en la conservación y custodia de la Historia Clínica y de acuerdo a las reglas de la Ley General de Archivo.

Política de seguridad y confidencialidad de la información

El HOSPITAL CIVIL DE IPIALES E.S.E., declara mediante la Política General de Seguridad y Privacidad de la información su posición con respecto a la protección de los activos de la información en su confidencialidad, integridad y disponibilidad, que soportan los procesos de la Entidad y apoya y garantiza los recursos para la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación, publicación y gestión de políticas específicas, lineamientos, procedimientos e instructivos, que permitan minimizar el impacto ocasionado por los riesgos de seguridad, privacidad y ciberseguridad de la información así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información. Todo esto en concordancia con la misión, visión, objetivos estratégicos de la entidad, los principios de la función pública, la mejora continua.

Activos de la información:

El hospital Civil de Ipiales realizó el levantamiento de los activos de la información en base a lo solicitado en el logro “Definición del marco de seguridad y privacidad de la información y de los sistemas de información”, contenido el autodiagnóstico de la política de gobierno digital, buscando con lo anterior proteger la información frente a la posible materialización de riesgos que afecten su disponibilidad, confiabilidad e integridad de la misma.

En esta matriz se buscó caracterizar los siguientes ítems:

Información básica: identificador: Número consecutivo único que identifica al activo en el inventario

Proceso: Nombre del proceso al que pertenece el activo.

Nombre del activo: Nombre de identificación del activo dentro del proceso al que pertenece.

Descripción/observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.

Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores: Información, Software, Recursos humanos, servicio, hardware, otro.

Tipo	**Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores.**
Información:	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
Software:	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
Recurso humano:	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
Servicio:	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
Hardware:	Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
Otros:	activos de información que no corresponden a ninguno de los tipos descritos anteriormente

	pero deben ser valorados para conocer su criticidad al interior del proceso.

Ubicación: de qué forma se encuentra el activo que toma los siguientes valores: física, electrónica o física y electrónica

Detalles de la ubicación: se detalla el sitio excepto del activo por ejemplo en un servidor, un archivo, oficina de algún proceso etc.

Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

CRITERIOS DE CLASIFICACION		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
IPR INFORMACION PUBLICA RESERVADA	**(A) ALTA**	**(1) ALTA**
IPC INFORMACION PUBLICA CLASIFICADA	**(M) MEDIA**	**(2) MEDIA**
IP INFORMACION PUBLICA	**(B) BAJA**	**(3) BAJA**
NC NO CLASIFICADA	**NC NO CLASIFICADA**	**NC NO CLASIFICADA**

ALTA	**Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.**
MEDIA	**Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.**
BAJA	**Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.**

Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

Propiedad: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

Acceso/usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Gestión/fecha de ingreso: Fecha de ingreso del activo de información en el inventario

Gestión/Fecha salida: Fecha de exclusión del activo de información del inventario.

Lo anterior va a permitir a la institución aplicar las siguientes actividades

- Verificar El nivel de entendimiento y aplicación de los lineamientos establecidos para garantizar la seguridad de la información en la Entidad u organismo.

- Aplicar medidas de seguridad implementadas para el procesamiento, acceso e intercambio de información.

- La evaluación continua y sistemática de los componentes.

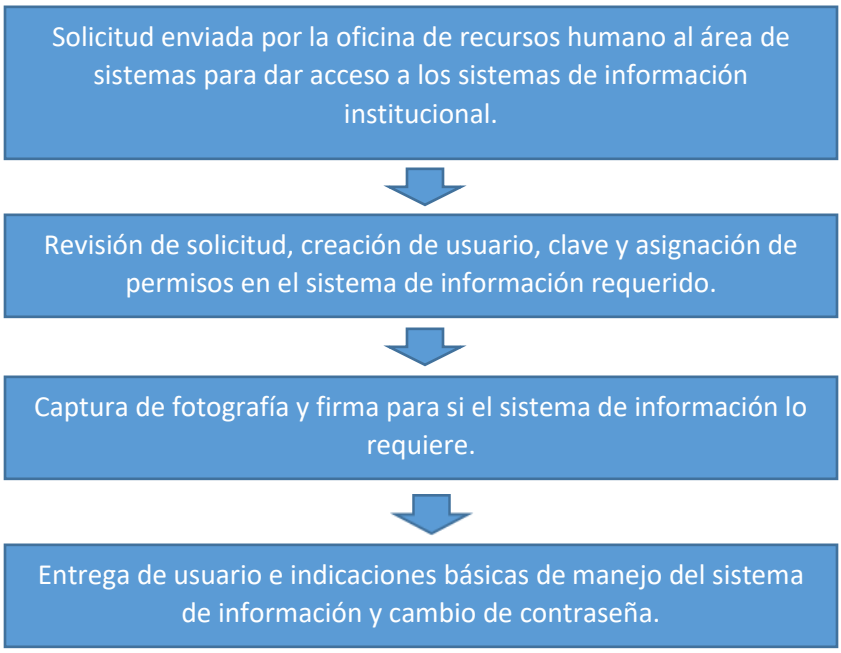
- La identificación de desviaciones y la definición de acciones de mejora.

Los activos de la información del hospital Civil de Ipiales están publicados en los siguientes enlaces:

https://hospitalcivilese.gov.co/site/index.php/informacion-al-ciudadano-2/10-instrumentos-de-gestion-de-la-informacion-publica/10-2-registro-de-activos-de-informacions de las

Asignación de usuario y cambio de contraseña:

Para la asignación de usuarios a los sistemas de información institucional, correo electrónico, páginas web para trámites administrativos, carpetas compartidas y demás aplicaciones con acceso restringido en el Hospital Civil de Ipiales se debe realizar los siguientes pasos:



El proceso de cambio de contraseña está a disposición de los usuarios en las diferentes aplicaciones y software de la institución, pero el área de sistema establece que este cambio se realice por lo menos cada seis meses, las claves de los servidores, correo electrónico cada tres meses, las carpetas compartidas y de ingreso a los equipos de cómputo anualmente, o a solicitud de los usuarios de estas, por otra parte la desactivación del usurario se la realiza al solicitar la firma del líder de sistemas en del FO 1378 “Formato de Paz y Salvo”

Asignación de usuario y contraseña para tener acceso remoto

El concepto de acceso remoto se refiere a la tecnología que permite a los funcionarios del Hospital civil de Ipiales acceder a los servicios o red institucional desde dispositivos que no se encuentran en el mismo entorno. Por definición, no requiere una conexión física entre las computadoras, ya que el proceso se realiza a través de una red virtual.

Para realizar este proceso el líder del proceso evalúa la necesidad de tener acceso remoto y la necesidad del funcionario que sea autorizado por subgerencia administrativa, ya que dentro de la institución los servicios no pueden paralizarse deben estar en funcionamiento las 24 horas del día los 7 días de la semana a los diferentes servicios como por ejemplo acceso al sistema de información hospitalaria, bases de datos servicios de laboratorio entre otros.

El líder del proceso realiza la solicitud formal a la Subgerencia Administrativa con copia al líder de la Gestión Tic y desde la oficina de sistemas se le asigna un usuario

y contraseña y se le realiza la instalación del escritorio remoto. Los funcionarios que tienen el acceso remoto se llena el registro en una hoja de cálculo Excel y su control de acceso desde un dispositivo microtik

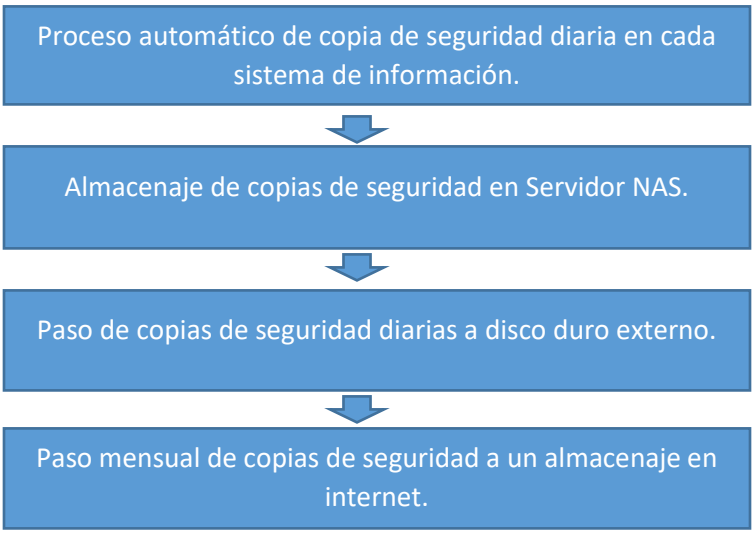
Copias de seguridad:

Desde el área de gestión TIC se tiene implementado el FO-0469 “Manejo de copias de seguridad” en cual se lleva el control de las copias de seguridad de las bases de datos del sistema de información del Hospital Civil de Ipiales:

	MANEJO DE COPIAS DE SEGURIDAD	FO – 0469	
		Versión: 2	Vigencia: 07/06/2017

RANGO DE FECHAS						MES	COPIA DE SEGURIDAD												
DESDE			HASTA				SISTEMA / SOFTWARE							MEDIO			No COPIAS	RUTA	NOMBRE DE COPIA
DIA	MES	AÑO	DIA	MES	AÑO		SIHOS	DARUMA	ANAR	EXABAN	AMSI	DGH	OTROS	MAGNETICO	SERVIDOR DE DATOS	OPTICO			

Estas copias de seguridad se ejecutan diariamente en los sistemas de información, dichas copias son enviadas a un servidor NAS destinado al almacenamiento masivo de información, seguido a esto se pasan las copias a un disco externo y una copia mensual es subida a una nube.



Las copias de seguridad de los equipos de cómputo de los procesos administrativos y asistenciales se realizan de acuerdo al cronograma de mantenimiento preventivo de equipos de cómputo, solicitud de los usuarios, mantenimiento correctivo que tenga que ver con formateo o reinstalación del sistema operativo, estas copias son almacenadas por un año en un servidor NAS al siguiente mantenimiento o copia,

esta será reemplazada previa concertación con el propietario de la información o líder del proceso, esto debido a que los equipos especialmente los administrativos contiene la mucha información la cual es imposible conservar en su totalidad.

También se tiene implementado un servicio de almacenaje en un servidor NAS de 14 TB con RAD 5, de información principal o importante según la documentación del proceso, decisión del personal de las oficinas o por trabajo técnico de las oficinas,

Antivirus:

La institución adquiere anualmente 400 licencias de antivirus ESET, software de seguridad informática que se utiliza para proteger los sistemas y dispositivos de los usuarios contra diferentes tipos de amenazas en línea, como virus, malware, spyware, ransomware, phishing y otras formas de ciberataques.

Detección en tiempo real de:

- Virus
- Troyanos
- Gusano
- Adware
- Spyware
- Phishing
- Aplicaciones potencialmente peligrosas
- Intrusiones por aplicaciones
- Plataforma de administración
- Actualización en línea

Se escoge este antivirus debido a su facilidad de uso y ofrece una protección confiable contra virus, además de consumir pocos recursos del equipo donde está instalado, también tiene una consola de administración con la cual se obtiene una

visión general de los equipos de cómputo, sus problemas y realizar acciones generales de mantenimiento.

5. MARCO CONCEPTUAL (DEFINICIONES RELEVANTES)

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos

de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en

el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública

- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales

- Ley 594 de 2000 - Ley General de Archivos

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica

- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales

- Ley 527 de 1999 - Ley de Comercio Electrónico

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley Estatutaria 1581 de 2012 - Protección de datos personales

- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información

7. DESCRIPCIÓN DEL PLAN

POLITICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

El equipo de colaboradores y el Gerente del Hospital Civil de Ipiales E.S.E. se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos de la información, fomento de canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendo con las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos de la institución.

OBJETIVOS DE LA POLITICA SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

- Garantizar la protección de datos personales de usuarios, clientes, proveedores y trabajadores tanto en los medios físicos como electrónicos.

- Controlar el uso efectivo de equipos de cómputo que garantice la confidencialidad, seguridad e integralidad de la información de los usuarios incluyendo.

- Fortalecer el conocimiento y la adherencia en el plan de contingencia en caso de caída del sistema de información

ALCANCE:

Esta política abarca los siguientes procesos:

ESTRATEGICO: TODOS LOS PROCESOS

MISIONAL: TODOS LOS PROCESOS

DE APOYO: TODOS LOS PROCESOS

El siguiente plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Para realizar este paso los responsables del plan deben efectuar la recolección de

la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del MSPI.

EJE ESTRATEGICO PLAN DE DESARROLLO	OBJETIVO ESTRATEGICO	FUENTE DE COMPROMISOS	DIMENSIONES DEL MIPG	POLITICA DE GESTION Y DESEMPEÑO INSTITUCIONAL	ALINEACION CON OTROS PLANES	PROCESO ASOCIADO	META	ACTIVIDADES PLANEADAS	
Realizar el diagnóstico de seguridad y privacidad de la información para la vigencia, constituyéndola a través de la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI)	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr el 100% del diagnóstico de seguridad y privacidad de la información**	**P**	Cronograma para el diagnóstico de seguridad y privacidad de la información
								H	Ejecutar el diagnostico de seguridad y privacidad de la información mediante la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI)
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Aprobación, implementación y actualización de la política de seguridad y privacidad de la información mediante el	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr el 100% de actualización de la política de seguridad y privacidad de la**	**P**	Elaborar un cronograma de capacitaciones y difusión de la política de seguridad y privacidad de la información para todos los colaboradores incluyendo los proveedores de servicios

proceso de mejora continua	**de servicios de salud con calidad, oportunidad, seguridad y humanización.**						**información mediante el proceso de mejora continua**		externos, contratistas y demás grupos de valor del hospital civil de Ipiales.
								H	Realizar capacitaciones y difusión de la política de seguridad y privacidad de la información para todos los colaboradores incluyendo los proveedores de servicios externos, contratistas y demás grupos de valor del hospital civil de Ipiales.
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Implementar procedimientos de seguridad y privacidad de la información aprobados y actualizados mediante un proceso de mejora continua	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr Implementar en un 80% los procedimientos de seguridad y privacidad de la información aprobados y actualizados mediante un proceso de**	**P**	Teniendo en cuenta el diagnóstico de seguridad y privacidad de la información mediante la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI) analizar que procedimientos de seguridad y privacidad se pueden implementar conjuntamente con el comité de seguridad y

							mejora continua		confidencialidad de la información aprobado mediante resolución No 3626 de 7 de dic de 2023
								H	Implementar procedimientos de seguridad y privacidad de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Actualización de los activos de la información mediante el proceso de mejora continua	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr la actualización del 100% de los conjuntos de datos mínimos que se publican en la página de datos abiertos mediante el proceso de mejora continua**	**P**	Elaborar un cronograma para la actualización de activos de la información vigencia 2025
								H	Realizar la actualización de activos de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados

Elaborar, aprobarlo e implementar un plan operacional de seguridad y privacidad de la información	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr un 50% la elaboración, aprobación e implementación del plan operacional de seguridad y privacidad de la información**	**H**	Elaborar del plan operacional de seguridad y privacidad de la información
								H	aprobar del plan operacional de seguridad y privacidad de la información
								H	implementar del plan operacional de seguridad y privacidad de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Actualizar y aprobar los indicadores midiendo la eficiencia y eficacia del sistema de seguridad y privacidad de la información	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr el 100% de actualización y aprobación de los indicadores midiendo la eficiencia y eficacia del sistema de seguridad y privacidad de la información**	**P**	Analizar los indicadores que actualmente de tiene para verificar la eficiencia y eficacia del sistema de seguridad y confidencialidad de la información
								H	Elaborar la actualización de los indicadores que midan la eficiencia y eficacia del sistema de seguridad y confidencialidad de la información
									aprobación de los indicadores que midan la eficiencia y eficacia del sistema de seguridad y

									confidencialidad de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados

8. BIBLIOGRAFÍA

Ministerio de las TCI

http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Ministerio de las TCI

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Escuela Tecnológica

http://www.itc.edu.co/es/nosotros/seguridad-informacion