
| Documentado. | | Revisado | Aprobado |
|---|---|---|---|
| **Nombre:** | **HEYNER AROCA ARAÚJO** | **COMITÉ DE GESTIÓN Y DESEMPEÑO** | **MAGRETH SÁNCHEZ BLANCO** |
| **Cargo:** | **PROFESIONAL UNIVERSITARIO SISTEMAS** | **MIEMBROS COMITÉ** | **PRESIDENTE COMITÉ MIPG** |
| **Firma:** | **P/D: Original Firmado** | **Acta No 5 del 30 de Enero de 2019** | **P/D: Original Firmado** |

## 1. INTRODUCCIÓN

Este documento busca lograr la implementación en la **ESE Hospital Rosario Pumarejo de López**, las mejoras prácticas dadas 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. Este plan aplica a todos los procesos de la institución los cuales manejan, procesos en la E.S.E.

## 2. GENERALIDADES:

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

### OBJETIVO GENERAL

Generar un documento institucional guiado en los lineamientos de buenas prácticas en seguridad y Privacidad de la información.

### OBJETIVO ESPECIFICO

- Promover el uso de mejores prácticas de seguridad de la información en la institución
- Optimizar la gestión de la seguridad de la información al interior de le entidad
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales
- Optimizar la labor de acceso a la información pública.

### PLATAFORMA ESTRATEGICA:

### MISIÓN.

Somos una Empresa Social del Estado prestadora de servicios de salud de mediana complejidad en el Departamento del Cesar y áreas de influencia, por tener un talento humano idóneo, comprometida con la satisfacción de las necesidades del usuario, su

familia, incluyente y participativa, fundamentada en la relación docencia servicio; respetuosa del entorno ambiental.

**VISIÓN.**

Nuestro hospital en el año 2020 será una institución de alta complejidad, líder en la prestación de servicios de salud, aplicando altos estándares de calidad con humanización, en búsqueda permanente de la excelencia.

**PRINCIPIOS Y VALORES:**

**Principios.**

El Hospital en el desarrollo de las acciones en salud ha fundamentado los siguientes principios que soportan su cultura organizacional y son la base del sistema de valores éticos adoptados por los servidores públicos de la entidad.

- **HUMANIZACION:** Trato con calidez y dignidad.
- **PERTINENCIA:** Atención científica con el mínimo riesgo de acuerdo a la necesidad.
- **OPORTUNIDAD:** Garantizar los servicios requeridos sin retraso.
- **INTEGRALIDAD:** Cobertura de las necesidades de salud y satisfacción del usuario.
- **TRABAJO EN EQUIPO:** Cooperación y armonía para el logro de objetivos.

**Valores.**

Los valores éticos se presentan y establecen de manera explícita así como a través de un compromiso de la fuerza laboral para consolidad la cultura organizacional. De esta forma, la creación de las estrategias habilitan las capacidades organizacionales con los clientes externos e internos a ella bajo la concepción de una filosofía de integralidad para mantener la identidad mediante una proyección ética. Es decir, cuanto mejor sea la relación entre estas actividades y características administrativas, más probables será que haya una ejecución estratégica visible para alcanzar un beneficio rentable. Pelekais y Caridad (2013), gestión del talento humano.

Los Valores que rigen la forma de actuar de los servidores públicos en esta Institución se describen a continuación:

- **HONESTIDAD:** Este valor busca en los servidores del Hospital generar confianza y credibilidad en la sociedad a través de comportamientos y actitudes íntegras y transparentes.

- **RESPETO:** Se busca en los servidores del hospital valorar sus fortalezas, tolerar sus debilidades y aceptar su forma de pensar y actuar.

- **DILIGENCIA:** cumplir con los deberes asignados funciones, responsabilidad con atención, prontitud y eficiencia para optimizar el uso de los recursos del estado

- **JUSTICIA:** actuar con imparcialidad garantizando los derechos de las personas con equidad, igualdad y sin discriminación.

- **SOLIDARIDAD:** Los servidores hospital desarrollan actitudes de fraternidad y ayuda mutua, promoviendo condiciones que permitan el crecimiento de las personas en todas las dimensiones posibles dentro de un ambiente de equidad y justicia social.

**TOLERANCIA:** Este valor busca que los servidores del hospital actúen respetando y aceptando las diferencias que caracterizan a las personas.

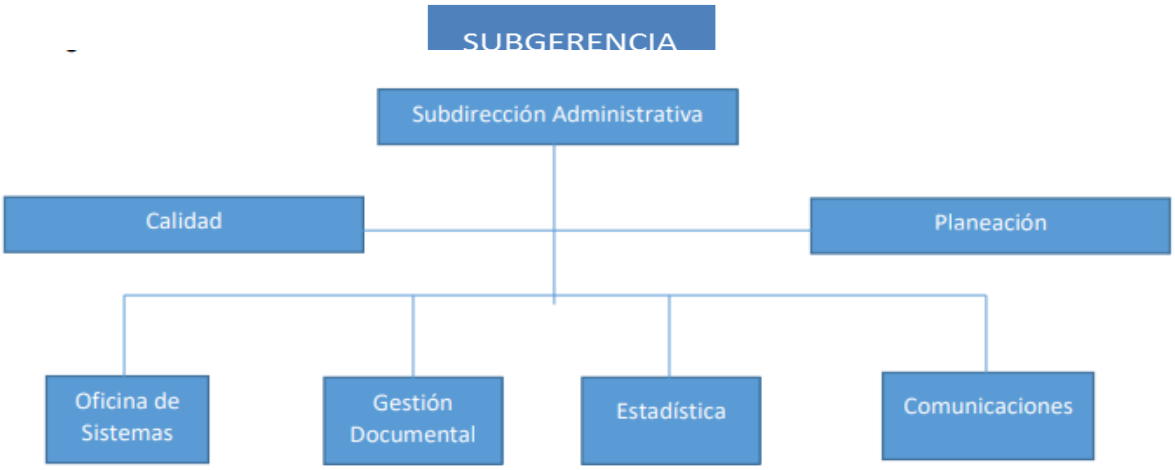
## ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

**ESTRATEGICO:** TODOS LOS PROCESOS
**MISIONAL:** TODOS LOS PROCESOS
**DE APOYO:** TODOS LOS PROCESOS

## 3. RESPONSABLES

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:




Subgerente Financiero
Profesional Universitario de Planeación
Profesional Universitario de Calidad
Ingeniero de Sistemas
Técnico en gestión documental
Profesional Especializada Estadística
SIAU

## 4. GLOSARIO.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**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.

**Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

## 5. ESARROLLO DEL PLAN.

### SEGURIDAD DE LA INFORMACIÓN:

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

**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.

**Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

### 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.

**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) para el cumplimiento de este articulo debe tenerse en cuenta los siguientes aspectos.

**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.

**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.

**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)

**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)

**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)

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).

**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.

**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.

**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.

**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.

**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).

**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.

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

**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.

**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.

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

**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
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

- 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
- 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
- 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.
- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
- 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

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.

## 7. DESCRIPCIÓN DEL PLAN

### POLITICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

El equipo de colaboradores y el Gerente del Hospital Rosario Pumarejo de López 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 DE GESTION DE CALIDAD

- 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

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 ejecutar este paso los responsables deben realizar 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.

| Nº DE ORDEN | CALIDAD ESPERADA | OPORTUNIDA DE MEJORA | PRIORIZACIÓN | | | | BARRERA DE MEJORAMIENTO Y CONTROL PROPUESTO | PHVA | ACCIONES DE MEJORAMIENTO | PESO % | PROCESO, PERSONA O GRUPO DE TRABAJO RESPONSABLE DE LA ACCIÓN DE MEJORA | PERIODO DE DESARROLLO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Riesgo | Costo | Volumen | Total | | | | | | |
| 1 | Plan de Seguridad informática realizado con todos sus ítems de manera real y conforme a las guías de MINTIC. | Plan de Seguridad informática incompleto, no cumple con las recomendaciones de las Guías de MINTIC en este tema | 5 | 5 | 5 | 125 | - Bajo conocimiento en la implementación de este tipo de planes<br>-'<br>Subjetividad en el levantamiento de la información | **P** | Definir cronograma de actividades para **identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información** incluyendo los ítem<br>Guía 1 - Encuesta de seguridad<br>Guía 2 - Estratificación<br>Guía 3 - Autodiagnóstico de cumplimiento de la ley de protección de datos personales<br>Guía 4 – Autoevaluación del Modelo de Seguridad de la Información | 10% | Proceso de gestión de la información | Año 2019 |
| | | | | | | | | **H** | Aplicar las guías según cronograma establecido | 60% | Proceso de gestión de la información | |
| | | | | | | | | **V** | Socializar los hallazgos encontrados a la alta dirección. | 20% | Proceso de gestión de la información - Subdirección Administrativa - Gerencia | |
| | | | | | | | | **A** | Realizar acciones según resultados de efectividad obtenidos | 10% | Proceso de gestión de la información – Subgerencia Financiera - Gerencia | |

## 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/artices-5482_Modelo_de_Seguridad_Privacidad.pdf

Escuela Tecnológica

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