

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 1 de 13

## 1. INTRODUCCIÓN

La ESE Hospital Rosario Pumarejo de López, reconoce la información como un activo importante para la atención de los pacientes y el desarrollo de sus procesos internos, por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para 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, integridad y disponibilidad de los datos. Este plan aplica a todos los procesos de la institución los cuales manejan, procesos en la E.S.E.

El plan contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en el Hospital Rosario Pumarejo de López E.S.E. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o transmitan información de la institución o sus pacientes.

## 2. 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.

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, tu familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 2 de 13

- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y 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 reforma 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.

### 3. OBJETIVOS

Establecer los lineamientos principales de gobierno y gestión de la seguridad de la información para el Hospital Rosario Pumarejo de López E.S.E.

#### 2.1. OBJETIVOS ESPECÍFICOS

- 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 la entidad y la labor de acceso a la información pública.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 3 de 13

## 4. ALCANCE

El plan contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en el Hospital Rosario Pumarejo de López. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todas las contrapartes que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

## 5. RESPONSABLES

Según la estructura orgánica de la institución, los responsables de la implementación del plan es la siguiente:

- Subgerente Administrativo y Financiero
- Asesor planeación, calidad y sistemas de información
- Profesional de apoyo calidad
- Prof. Universitario - Sistemas
- Líder en gestión documental
- Profesional Especializado Estadística
- Profesional líder de SIAU
- Líderes de procesos

## 6. 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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.

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

**Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional,

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 4 de 13

operativa y administrativa de cada entidad, órgano u organismo.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para el Hospital Rosario Pumarejo de López.

**Comité de Seguridad de la Información (CSI):** Instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público. Para la E.S.E. Hospital Rosario Pumarejo de López, se tiene el Comité Institucional de Gestión y Desempeño, el cual asume a través de la dimensión de Información y Comunicación, las funciones del CSI.

**Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

**Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

**Evento de seguridad de la información:** Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

**Incidente de seguridad de la información:** Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información de Hospital Rosario Pumarejo de López y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

**Propietario/responsable de activo de información:** Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 5 de 13

**Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

**Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

## 7. DESARROLLO 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 (Gobierno en línea) 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 artículo 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)

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 6 de 13

**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, art3).

**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

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 7 de 13

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.

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 8 de 13

**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, anonimizarían o cifrado.

**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.

**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 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.

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

**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

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 9 de 13

inequívoco a un individuo o entidad.

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

## 8. DESCRIPCIÓN DEL PLAN

### 8.1. POLÍTICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La Junta Directiva o quien haga sus veces, el gerente y el equipo de colaboradores del Hospital Rosario Pumarejo de López E.S.E., se comprometen a garantizar la confidencialidad, seguridad e integridad 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.

### 8.2. OBJETIVOS DE LA POLÍTICA DE 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 integridad 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
- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, 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.

## RECURSOS

**Humanos:** Gerente, funcionarios y contratistas de la E.S.E. Hospital Rosario Pumarejo de López

**Físico:** PC y equipos de comunicación

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 10 de 13

## METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la E.S.E Hospital del Rosario, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPi:

- Diagnosticar o Planear
- Hacer
- Verificar
- Actuar



*Fuente: Modelo De Seguridad Y Privacidad De La Información Emitida Por Mintic*

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida NIT: 892399994-5</p>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b>	FECHA	31/01/2024
		HOJA	Página 11 de 13

## ACTIVIDADES

### 1. Realizar Diagnóstico

Se realizará diagnóstico aplicando los instrumentos dispuestos por Mintic

METAS/ACTIVIDADES	ENTREGABLES	CUMPLIMIENTO	PERIODO DE DESARROLLO	RESPONSABLE
Realizar el diagnóstico del estado actual de gestión de seguridad y privacidad de la información	Documento diagnóstico del estado actual	100%	Primer semestre 2024	Profesional universitario de sistemas
Manual Catálogo de servicios TIC	Documento con el catálogo de software que posee la entidad	100%	Primer semestre 2024	Profesional universitario de sistemas
Implementar controles de seguridad de accesos remotos de usuarios	Procedimiento de acceso remotos elaborado y aprobado	100%	Toda la vigencia 2024	Profesional universitario de sistemas
Capacitación de seguridad y privacidad de la información	Listado de asistencia de la capacitación, medido por talento humano asistente/talento humano convocado	100%	Toda la vigencia 2024	Profesional universitario de sistemas
Actualización de la política de seguridad de la información	Documento actualizado de la política aprobada	100%	Toda la vigencia 2024	Profesional universitario de sistemas

- a. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- b. Realizar la Identificación de los Riesgos con los líderes del Proceso.
- c. Entrevistar con los líderes del Proceso.

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 12 de 13

## 2. Planificación.

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar (Ajustar) el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

### **CUMPLIMIENTO DE IMPLEMENTACIÓN**

La ESE de acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el la E.S.E Hospital del Rosario o Aspectos organizativos de la seguridad de la información o Seguridad Ligada a los recursos humanos

- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información

### **SEGUIMIENTO y EVALUACIÓN**

La ESE al finalizar cada etapa se realizará una reunión para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

### **ENTREGABLES**

- Informe de avance o resumen ejecutivo
- Acta de Reunión.
- Plan de tratamiento de riesgo o Política de Seguridad Ajustado.
- Productos de cada etapa

 <p>EMPRESA SOCIAL DEL ESTADO <b>HOSPITAL</b> ROSARIO PUMAREJO DE LÓPEZ Por ti, familia y la vida</p> <p>NIT: 892399994-5</p>	<p><b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b></p>	CÓDIGO	GTI-PL-001
		VERSIÓN	002
	<p><b>PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN</b></p>	FECHA	31/01/2024
		HOJA	Página 13 de 13

## 9. CONTROL DE CAMBIOS

VERSIÓN	FECHA LIBERACIÓN DOCUMENTO			MOTIVO DEL CAMBIO
	DIA	MES	AÑO	
001	30	01	2023	Actualización de documento en contenido y normatividad vigente, así mismo, se actualiza codificación y versión toda vez que se incorpora en el listado maestro de control documental del SIGC.
002	31	01	2024	Actualización del documento, cambio de vigencia

	ELABORO:	REVISO:	APROBO:
<b>NOMBRE</b>	Miguel Ángel Rodríguez Herazo	William Humberto Salgado Gamboa	Duver Dicson Vargas Rojas
<b>CARGO</b>	Profesional Universitario de sistemas	Subgerente Administrativo y Financiero	Agente Especial Interventor
<b>FIRMA</b>			