

	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 1 de 11

1. INTRODUCCIÓN:

La E.S.E. Hospital Rosario Pumarejo de López, en cabeza de la Gerencia ha venido realizando fortalecimiento de la gestión de TI de la entidad, implementando nuevas herramientas y fortaleciendo la parte tectológica en la compra de nuevos y modernos equipos con el fin de ampliar la capacidad de la infraestructura tecnológica e implementando el modelo de seguridad digital, acatando las recomendaciones y lineamientos establecidos desde el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Entendiendo la importancia de una buena gestión de seguridad de la información, se han venido desarrollando y documentando los procesos de implementación de un sistema de gestión de seguridad de la información conforme al Modelo de Seguridad y Privacidad de la Información establecido por la Política de Gobierno Digital, buscando establecer un marco de confianza en el ejercicio de las actividades diarias de los usuarios y los ciudadanos y que valla acorde a nuestra misión y visión institucional.

Para la E.S.E. Hospital Rosario Pumarejo de López, la protección de la información busca la disminución de riesgo en pérdida o fuga de datos que llegue a causar un impacto negativo para la entidad y se vea afectado la prestación de los servicios a todos nuestros usuarios y pacientes.

2. OBJETIVO:

Realizar y promover una política de seguridad de la información para las buenas prácticas y uso de la información generada en la E.S.E. Hospital Rosario Pumarejo de López generada.

3. ALCANCE:

Este documento tiene como alcance la elaboración y socialización de la política de seguridad y privacidad de la información en la E.S.E. Hospital Rosario Pumarejo de López basado en el Modelo de Seguridad y Privacidad de la Información en el marco de la Estrategia de Gobierno en Línea.

4. RESPONSABLES:

Entiéndase como responsable de la información, toda persona que emita cualquier documento que haga parte de la gestión asistencial y administrativa dentro de la organización.

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 2 de 11

Rol administrador: persona encargada de administrar, custodiar y verificar las copias de seguridad del sistema de información.

Rol estándar: persona que produce y/o emite cualquier información de ende administrativo y asistencial en a la institución.

5. MARCO NORMATIVO:

La E.S.E. Hospital Rosario Pumarejo de López, como entidad pública, al igual que cualquier organismo del estado, se encuentra cubierta por un marco normativo y regulatorio en todo lo relacionado con la seguridad de la información, como también un marco estipulado por MINTIC.

Para el desarrollo de una política de Seguridad de la información se tiene en cuenta la Estrategia de Gobierno Digital, que se evidencia en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, que comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea optima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información.

A continuación, se relacionan las demás normas, leyes, decretos y resoluciones que aplican para el hospital en implementación y operación del SGSI:

- NTC-ISO/IEC 27001- 27002
- Decreto 2693 de 2012 MinTic
- Decreto 1008 de 2018 MinTic.
- Decreto 1414 de 2017 de MinTic.
- Ley 1712 de 2014
- Ley 1273 de 2009
- Decreto 1078 de 2015 MinTic
- Ley 1581 de 2012.
- Decreto 415 de 2016 MinTic
- Decreto 1377 de 2013
- Ley 1266 de 2008

6. GLOSARIO:

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 3 de 11

la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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).

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.

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 4 de 11

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 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, art6)

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 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).

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

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 5 de 11

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)

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.

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).

7. POLÍTICAS:

Políticas de Seguridad y privacidad de la información.


Se define la Política de Seguridad de la Información como la manifestación que hace la gerencia de la E.S.E Hospital Rosario Pumarejo de López, sobre la intención institucional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad y privacidad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus datos.

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, tu Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 6 de 11

La E.S.E Hospital Rosario Pumarejo de López pretende mediante la adopción e implementación de un Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y autenticidad de la información.

La E.S.E Hospital Rosario Pumarejo de López se compromete a implementar un sistema de gestión de la seguridad de la información llevando a cabo los siguientes compromisos:

- ✓ La gestión de los riesgos de los activos de información teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.
- ✓ Una gestión integral de riesgos basada en la implementación de controles físicos y digitales orientadas a la prevención de incidentes.
- ✓ El fomento de la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados por medio de una obligación contractual de confidencialidad de la información.
- ✓ Se mitigarán los incidentes de Seguridad y Privacidad de la Información, mediante un procedimiento de resguardar la información a través de un backups diario del sistema de información.
- ✓ Se generará conciencia para el cambio de claves de cada uno de los usuarios fomentando así las buenas prácticas de seguridad.
- ✓ Se protegerá las instalaciones de software no autorizado por la entidad en cada uno de los equipos institucionales. y la infraestructura
- ✓ Se implementará control de acceso a la información, sistemas de información a través de la creación de usuarios y asignación de roles a cada uno de los usuarios.

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 7 de 11

Deberes individuales de los usuarios de la información

- Usar la información del hospital solamente para propósitos de vayan de acuerdos a la actividad económica de la entidad.
- Respetar la confidencialidad de la información financiera y asistencia de la institución.
- No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial.
- Devolver y no conservar ningún tipo de copia de información una vez termine su vínculo laboral con la Entidad
- Esta estrictamente prohibido la divulgación, cambio, retiro o perdida no autorizada de información de la Entidad almacenada en medios físicos removibles, como USB, CD, DVD y Discos duros personales.
- Esta estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos de la entidad, copiar software licenciado de la E.S.E Hospital Rosario Pumarejo de López, para utilizar en computadores personales, ya sea en su domicilio o en cualquier otra instalación sin autorización de jefes de áreas y oficina de sistemas.
- Cuando un contratista se ausenta de su trabajo por un periodo de tiempo superior a 5 días hábiles o se da por terminado la vinculación laboral, su supervisor debe de forma inmediata:
 - a. Suspensión de los accesos a los recursos físicos y a la información institucional
 - b. Notificar la fecha en que el acceso debe ser suspendido, de ser necesario.
 - c. Recoger los equipos de seguridad como por ejemplo llaves, claves, computadoras, etc y entregar a la oficina de activos fijos.

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, tu Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 8 de 11

8. LINEAMIENTOS GENERALES PARA EL CUMPLIMIENTO DE LA POLITICA:

Uso adecuado de Software.

- ✓ En las estaciones de trabajo del hospital solo se puede instalar software desarrollado o adquirido legalmente y cuya licencia de uso este a nombre de la E.S.E Hospital Rosario Pumarejo de López.
- ✓ La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones de trabajo es del equipo de trabajo de de la oficina de sistemas del hospital.
- ✓ Las estaciones de trabajo de hospital deben ser utilizadas por los empleados o contratistas solo para el desarrollo de las funciones normales de su trabajo.
- ✓ Los usuarios deben cumplir con la Legislación Colombiana que regula los derechos de autor.

Control de Virus.

- ✓ Los computadores personales deben mantener activo un software antivirus, Sistema Operativo, Microsoft Office, licenciados y Actualizados y que su uso haya sido Autorizado por su jefe inmediato y la oficina de sistema del hospital.
- ✓ Los servidores de la institución deberán mantener activo un software antivirus licenciado.
- ✓ Los computadores personales y servidores deben ser analizados contra virus periódica y automáticamente.
- ✓ Cualquier información que venga por medio electrónico o magnético como correo electrónico o información de INTERNET, debe ser revisada por un software antivirus antes de ser descargada y utilizada.
- ✓ Es responsabilidad de los usuarios reportar todos los incidentes de infección de virus a las áreas encargadas.
- ✓ Es responsabilidad de los usuarios tomar copias de la información y verificar que el respaldo esté libre de cualquier infección de virus.
- ✓ El usuario debe asegurar que toda la información que provenga de fuentes conocidas.

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, tu Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 9 de 11

Control de contraseñas.

- ✓ Los perfiles de usuario y la contraseña tienen que ser asignados individualmente para soportar el principio de responsabilidad individual.
- ✓ Los usuarios no pueden prestar su contraseña y el que lo realice con su perfil queda bajo la responsabilidad del dueño.
- ✓ El usuario no debe compartir, escribir o revelar su contraseña.
- ✓ La oficina de sistemas le asignará una clave genérica y cada usuario deberá realizar el cambio de la misma y queda bajo su responsabilidad el no asignar una nueva clave.

Copias de respaldo de información (Backups), ver procedimiento :

- ✓ Se debe contar con un sistema automático para la recolección de copias de respaldo.
- ✓ Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
- ✓ Los medios magnéticos o digitales que contienen información deben ser almacenados en lugares seguros y bajo la custodia de la persona responsable de la oficina de sistemas.
- ✓ Los usuarios responsables por respaldar la información también son responsables de facilitar la oportuna restauración de la información por lo menos una vez a la semana.
- ✓ Se debe mantener respaldos de la información guardados en intervalos de 10 días para que en caso de contingencia se pueda recuperar la información oportunamente. Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos. A través de la herramienta de google DRIVE que es una de las licencias activas que tiene adquirida el hospital.

9. ETAPAS PARA LA IMPLEMENTACIÓN:

- 1. Desarrollo de las políticas:** En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, tu Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 10 de 11

requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

- a. **Justificación de la creación de política:** definido en el numeral 7 del documento.
 - b. **Alcance:** definido en el numeral 3 del documento.
 - c. **Roles y Responsabilidades:** definido por el numeral 4 del documento.
 - d. **Revisión de la política:** la revisión de esta política la realizará la oficina de planeación y será aprobada por la gerencia.
 - e. **Aprobación de la Política:** Se debe determinar al interior de la entidad la persona o rol de la gerencia que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de esta.
2. **Cumplimiento:** Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.
 3. **Comunicación** la divulgación de esta política se realizará por medio de la página web de la institución.
 4. **Monitoreo:** Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de estas, por lo cual se realizara por medio de las planillas digitales donde se reportaran las actividades a realizar.
 5. **Mantenimiento:** se realizará evaluaciones cada 6 meses a los usuarios del sistema de información para saber si está siendo efectiva la política o necesita ajustes.

DOCUMENTOS DE REFERENCIA:

- <https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla>
- https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf
- https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf
- https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

 <p>EMPRESA SOCIAL DEL ESTADO HOSPITAL ROSARIO PUMAREJO DE LÓPEZ Por ti, tu Familia y la Vida NIT: 892399994-5</p>	MANUAL DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GTI-MA-001
		VERSIÓN	001
	PROCESO: GESTIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN	FECHA	26/10/2022
		HOJA	Página 11 de 11

CONTROL DE CAMBIOS:

VERSIÓN	FECHA LIBERACIÓN DOCUMENTO			MOTIVO DEL CAMBIO
	DIA	MES	AÑO	
001	26	10	2022	Documento nuevo

	ELABORO:	REVISO:	APROBO:
NOMBRE	MIGUEL ANGEL RODRIGUEZ HERAZO	ERIKA GIOVANNA DÍAZ LONDOÑO	DUVER DICSON VARGAS ROJAS
CARGO	Profesional Universitario de sistemas	Profesional Especializado Apoyo en Planeación (C)	Agente Especial Interventor
FIRMA			
FECHA	26-10-2022	26-10-2022	26-10-2022