

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL GARZÓN - HUILA NIT: 891.180.026-5	Código:
		Versión: 02
	POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	Vigencia: 00/00/2017

POLITICA DE SEGURIDAD DE LA INFORMACION

1. INTRODUCCIÓN

La E.S.E Hospital Departamental San Vicente de Paúl de Garzón, reconoce la información como uno de sus activos más importantes para la atención de los pacientes y el desarrollo e innovación de sus procesos internos, por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para mantener y preservar la información.

Esta política es un documento que contiene los lineamientos que apoyan la gestión y administración de los planes y procedimientos respecto a la “Seguridad de la Información” dando claridad sobre las buenas prácticas de seguridad aplicadas a la institución.

2. JUSTIFICACIÓN DE LA POLÍTICA

Con el fin de garantizar los principios de confidencialidad, integridad y disponibilidad en la información que se maneja al interior de la E.S.E Hospital Departamental San Vicente de Paúl, tanto en medio físico como magnético, se dicta como política de seguridad de la información, la serie de lineamientos que todos los funcionarios y colaboradores de la institución deben cumplir y que incluyen:

- ✓ Uso adecuado de la infraestructura y tecnología dispuesta para el manejo de la información.
- ✓ Respeto por las disposiciones relacionadas con la seguridad de la información.
- ✓ Respeto por las restricciones de acceso definidas en los diferentes procesos de manejo de la información.
- ✓ Compromiso de informar al departamento de las TICS del Hospital, cuando se sospeche o se tenga conocimiento de hechos que pongan en riesgo la seguridad de la información.

3. SITUACIÓN DESEADA

Compromiso con el Buen Uso de la Tecnología Informática y la Seguridad de la Información

4. CONTEXTO DE LA POLITICA:

4.1. MARCO LEGAL

Para la construcción de esta política se tiene como base, la norma ISO/IEC 27001, tecnología de la Información, técnicas de seguridad y sistema de gestión de la seguridad de la información y las siguientes normas:

Norma	Entidad que la expidió	Asunto
Ley 1712 de 2014	El congreso de la república.	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1581 de	El congreso de la república	Por la cual se dictan disposiciones generales

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL GARZÓN - HUILA NIT: 891.180.026-5	Código: Versión: 02
	POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	Vigencia: 00/00/2017

2012		para la protección de datos personales
Ley 1341 de 2009	El congreso de la república	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones
Ley 527 de 1999	El congreso de la república	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Decreto 103 de 2015	El Presidencia de la Republica de Colombia	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 2578 de 2012	El Presidencia de la Republica de Colombia	Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto número 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del Estado
Decreto 2609 de 2012	El Presidencia de la Republica de Colombia	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 2573 de 2014	El Presidencia de la Republica de Colombia	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Resolución 1995 de 1999	El ministerio de salud	Por la cual se establecen normas para el manejo de la Historia Clínica.

4.2. MARCO SITUACIONAL

La información es un recurso que, como el resto de los activos, tiene un altísimo valor para la E.S.E y por consiguiente debe ser debidamente protegida. Se hace necesario el establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información que garantice un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones de la entidad apoyadas en un correcto sistema de información.

La institución establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL GARZÓN - HUILA NIT: 891.180.026-5	Código:
	POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	Versión: 02 Vigencia: 00/00/2017

Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

4.3. MARCO CONCEPTUAL

En la actualidad garantizar un nivel de protección total es virtualmente imposible, la seguridad de la información en la práctica a un nivel total o de completitud no es alcanzable porque no existe un sistema seguro al ciento por ciento. La información está expuesta a un mayor rango de amenazas y vulnerabilidades, porque “La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo de conversación”. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información protege a una organización que la adopte como parte de su visión y misión de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los posibles daños y maximizar el retorno de las inversiones y oportunidades. La información digital o en papel y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización. Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

5. TERMINOS Y DEFINICIONES:

Se presentan algunas definiciones importantes relacionadas al PSI (Política de Seguridad de la Información) que se busca diseñar:

- ✓ **Información:** Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- ✓ **Información Sensible:** Son todos aquellos archivos digitales generados desde los sistemas de información con los cuales la Institución cuenta
- ✓ **Seguridad:** Es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recursos humanos integrado para proveer toda la protección debida y requerida a la información y a los recursos informáticos de la entidad.
- ✓ **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.
- ✓ **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, operativa y administrativa de la entidad.
- ✓ **Copia de Seguridad. (BACKUP):** Se define como Backup o copia de seguridad, la actividad de resguardar de forma segura la información contenida en un medio de almacenamiento de origen (disco duro) a un medio de almacenamiento de destino de diferente tipo (otro disco duro, servidor de Backup, USB, CD, DVD, ZIP, entre otros)
- ✓ **Incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y gestionar los fallos de seguridad de la información. (ISO/IEC 27001)

Pág.3/6

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL GARZÓN - HUILA NIT: 891.180.026-5	Código:
		Versión: 02
	POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	Vigencia: 00/00/2017

6. MARCO GENERAL DE LA POLÍTICA

6.1. PROPÓSITO

La empresa social del estado Hospital Departamental San Vicente de Paúl manifiesta su compromiso con garantizar el cumplimiento de la norma que regula la gestión de la seguridad de la información, a través de las buenas practicas obteniendo los más altos niveles de seguridad, ofreciendo exactitud, disponibilidad e integridad y aprovechando las nuevas tecnologías de tal manera que contribuya a mejorar la accesibilidad, la claridad y el despliegue de la información a la hora que lo requiera cualquier usuario.

6.2. PRINCIPIOS

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Disponibilidad

6.3. OBJETIVOS:

6.3.1.GENERAL

Establecer los lineamientos principales del gobierno y gestión de la seguridad de la información para la E.S.E Hospital Departamental San Vicente de Paúl de Garzón.

6.3.2.ESPECÍFICOS

- ✓ Realizar actividades de seguimiento y control para verificar la aplicación de las políticas y normas que rigen los procesos de seguridad de la información.
- ✓ Implementar herramientas de seguridad informática que permitan proteger la información almacenada.
- ✓ Promover la gestión ética de la información y la confidencialidad de los datos derivados de las atenciones en salud.

6.4. METAS

- ✓ Definir y desarrollar la política de seguridad de la información en la E.S.E
- ✓ Desarrollar buenas prácticas que permitan la acreditación y liderazgo en dicho tema.
- ✓ Establecer una cultura informática, manejo y cuidado de la información.

6.5. ESTRATEGIAS

- ✓ Educación (Capacitaciones)

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL GARZÓN - HUILA NIT: 891.180.026-5	Código:
	POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	Versión: 02 Vigencia: 00/00/2017

- ✓ Controles y Auditorias
- ✓ Comunicación
- ✓ Evaluaciones

6.6. LÍNEAS DE INTERVENCIÓN Y ACTIVIDADES

- Fortalecimiento tecnológico
- Sensibilizar a los colaboradores de la ESE.

6.7. ABORDAJE DE RIESGOS Y OPORTUNIDADES

- ✓ Recurso Tecnológico
- ✓ Desconocimiento
- ✓ Resistencia al Cambio
- ✓ Falta de Disposición

6.8. DEFINICIÓN DE ROLES Y RESPONSABILIDADES

Estrategia	Responsable(s)	Rol
Capacitaciones	Líder de la política institucional de Seguridad de la Información	Capacitador
Auditorias	Líder de la política institucional de Seguridad de la Información	Auditor
Evaluaciones	Líder de la política institucional de Seguridad de la Información	Evaluador

6.9. MECANISMOS DE SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

- ✓ Encuestas
- ✓ Check List

6.10. INDICADORES DE SEGUIMIENTO A LOS OBJETIVOS ESTABLECIDOS EN LA POLÍTICA

- Porcentaje de cobertura de mecanismos de seguridad de la información.

6.11. MEJORA

Teniendo en cuenta los resultados de la medición de la cobertura de mecanismos de seguridad de la información, se implementarán los planes de mejora correspondientes.

7. PLANIFICACIÓN DE LOS CAMBIOS

Fecha	Cambio	Nueva Versión

8. APROBACIÓN

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL GARZÓN - HUILA NIT: 891.180.026-5	Código:
	POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	Versión: 02 Vigencia: 00/00/2017

9. REFERENCIAS BIBLIOGRÁFICAS