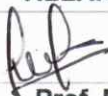
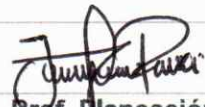
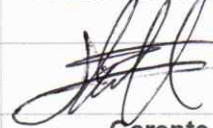


	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 1 de 13

POLÍTICA DE SEGURIDAD DIGITAL

NOMBRE	ELABORÓ	REVISÓ	APROBÓ
	LUISA FERNANDA MARTINEZ VILLARREAL	JHON FREDY REINA	CRISTIAN DANIEL AREVALO GUERRA
FIRMA			
CARGO	Prof. MIPG	Prof. Planeación	Gerente

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
 www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 2 de 13

TABLA DE CONTENIDO

1. JUSTIFICACIÓN.....	4
2. ALCANCE.....	4
3. OBJETIVOS DE LA POLITICA.....	4
3.1. OBJETIVO GENERAL	4
3.2. OBJETIVOS ESPECIFICOS.....	4
4. NIVEL DE CUMPLIMIENTO	5
5. APLICABILIDAD	5
8. TERMINO DE REFERENCIA.....	7
7. MARCO NORMATIVO	8
8. POLITICA DE SEGUIRAD DIGITAL	9
9.1 IMPLIMENTACION DE LA POLITICA	10
10 RESULTADOS ESPERADOS DE LA POLITICA	11
11. BIBLIOGRAFIA	13

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 3 de 13

INTRODUCCIÓN

A partir del artículo 133 de la Ley 1753 de 2015 y del Decreto 1499 de 2017, el Modelo Integrado de Planeación y Gestión -MIPG integró los sistemas de gestión de la calidad de la Ley 872 de 2003 y de Desarrollo Administrativo de que trataba la Ley 489 de 1998 y fueron derogados los artículos del 15 al 23 de la Ley 489 de 1998 y la Ley 872 de 2003.

MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de la ciudadanía, con integridad y calidad en el servicio.

Entre los objetivos de la puesta en marcha de MIPG se destaca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna.

De acuerdo con lo dispuesto en la política de SEGURIDAD DIGITAL, liderada por el Ministerio de las Tecnologías y las Comunicaciones – MinTIC y reglamentada bajo el decreto 1008 de 2018, la entidad busca, no solo que el uso de la tecnología sea ágil, sencillo y útil para las personas, sino también que la interacción entre los diferentes actores involucrados en la política se dé en medio de un ambiente seguro, corresponsable y previsible. Esta política incluye como un habilitador de la misma la seguridad de la información, junto con la arquitectura y los servicios ciudadanos digitales.

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 4 de 13

1. JUSTIFICACIÓN

Adoptar la Política de Seguridad Digital, el cual tiene como objeto fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital en la ESE Hospital Sagrado Corazón de Jesús.

2. ALCANCE

La Política de Seguridad Digital, busca proteger la información, minimizar los riesgos y asegurar la continuidad del servicio en de la Empresa Social del Estado, aplica a todos Servidores Públicos y en general todas aquellas personas naturales y jurídicas, que realicen cualquier actividad en la Empresa.

Este componente se desarrolla, a través de lineamientos en materia de seguridad digital, los cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos.

3. OBJETIVOS DE LA POLITICA

3.1. OBJETIVO GENERAL

Definir los lineamientos para identificar, gestionar, tratar y mitigar los riesgos y amenazas que puedan afectar la seguridad digital y el uso de las TIC en la en la ESE Hospital Sagrado Corazón de Jesús.

3.2. OBJETIVOS ESPECIFICOS

- ✓ Establecer las herramientas institucionales para la identificación, valoración, y tratar de mitigar los riesgos de seguridad digital.

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 5 de 13

✓ Garantizar en un grado la disponibilidad, integridad y confidencialidad de la información digital.

✓ Implementar el plan de capacitación y sensibilización con la finalidad de crear una cultura de seguridad institucional por medio de la aplicación de la normatividad vigente y de la adopción de buenas prácticas.

4. NIVEL DE CUMPLIMIENTO

La Política de seguridad digital, será de obligatorio cumplimiento para todos los funcionarios y contratistas que prestan sus servicios a la ESE HOSPITAL SAGRADO CORAZÓN DE JESÚS, independientemente de su tipo de vinculación.

5. APLICABILIDAD

La política de seguridad digital, es una política transversal por lo tanto será aplicable a los todos los servidores de la E.S.E. Hospital Sagrado Corazón de Jesús. La responsabilidad de los servidores públicos y demás colaboradores es llevar a cabo las directrices planteadas en esta política, dando a conocer la aplicación e implementación de lo aquí definido. Es un compromiso y responsabilidad de todos conocer la Política y es deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta.

6. TERMINOS DE REFERENCIA

- **Activo de Información:** Es todo aquello que en la Entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 6 de 13

- ***Carpetas Compartidas:*** Es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- ***CAU:*** Es el único Centro de Atención al Usuario en donde el grupo TIC presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TIC en la ESE Hospital Sagrado Corazón de Jesús
- ***Confidencialidad:*** La información no se pone a disposición ni se revela a individuos, Entidades o procesos no autorizados.
- ***Copias de respaldo:*** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- ***Dato:*** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- ***Disponibilidad:*** Acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, Entidades o procesos autorizados cuando lo requieran.
- ***Drive:*** Sitio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.
- ***Información:*** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- ***Información confidencial o crítica:*** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en la institución
- ***Integridad:*** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 7 de 13

- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
- **OTSI:** Oficina de Tecnología y Sistemas de Información.
- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones

De acuerdo al diagnóstico que se realiza a la política de seguridad digital, se puede evidenciar que se debe priorizar las actividades más importantes para el cumplimiento de los objetivos y metas de la E.S.E.

7. MARCO NORMATIVO

A continuación, se enuncian algunas de las normas que regulan la planificación institucional para asegurar una gestión integral eficiente, eficaz y transparente que evidencie cambios substanciales en el accionar de la entidad hacia la comunidad educativa y fuera de ella generando impacto en el territorio insular. Entre las cuales se encuentran:

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 8 de 13

- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- **Decreto 454 del 21 de marzo de 2020.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.
- **Decreto 1287 del 24 de septiembre de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Decreto 338 de 2022:** “Por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital”.
- **Directiva Presidencial 03 de 15 de marzo de 2021:** Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.
- **Ley Estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Resolución 500 de 2021:** “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- **Constitución política de Colombia 1991, Artículo 1:** Define a la intimidad y al buen nombre.
- **Decreto 2693 de 2012:** Estrategia de gobierno en línea. Ministerio de tecnologías de la información y las comunicaciones.
- **DECRETO 2364 DE 2012:** Firma electrónica

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 9 de 13

- **LEY 962 DE 2005.** Simplificación y realización de trámite. Atributos de seguridad en la información electrónica de entidades públicas.

8. POLITICA SEGURIDAD DIGITAL

La presente política tiene como finalidad una adecuada gestión de la información, buscando establecer un marco de confianza en el ejercicio de sus deberes para con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Por medio de la Política de Seguridad digital, tiene como objetivo definir los lineamientos para preservar la integridad, disponibilidad y confidencialidad de la información conforme al cumplimiento de los requisitos legales, estratégicos, operativos, tecnológicos y tácticos, aplicando las buenas prácticas de seguridad de la información digital.

Fortalecer la participación en la mejora de las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso de seguridad digital convocadas por la ESE Hospital sagrado corazón de Jesús.

La ESE Hospital sagrado corazón de Jesús, está comprometida en garantizar el tratamiento de los datos personales, por lo cual se acoge a las disposiciones contenidas en la Ley 1581 de 2012 y la Política de Tratamiento de Datos Personales, que tiene por objetivo establecer los criterios bajo los cuales se recolectan, almacenan, usan, circulan y suprimen los datos personales tratados así como el procedimiento para la garantía de los derechos de los titulares de los datos personales.

La tercera línea de defensa está a cargo de la oficina de control interno, quienes realizan la auditoria de seguimiento a los planes de acción, verificando el cumplimiento de los lineamientos establecidos.

9. IMPLEMENTACIÓN DE LA POLITICA

La implementación de la política por parte de la Empresa Social del Estado Hospital Sagrado corazón de Jesús , se hará a través de la adopción e implementación de lo exigido por el MinTIC quien elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, proteger y darle seguridad a la información , el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales,

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 10 de 13

técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información.

Fase: 1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción de la política de seguridad digital. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

Fase 2. Planificación: Determinar las necesidades y objetivos de seguridad digital teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo, para a elaborar el Plan de Seguridad digital.

Fase 3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Fase 4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción de la política de seguridad digital.

Fase 5. Mejoramiento Continuo: Establecer procedimientos para identificar falencias y mejorar el proceso continuo de la política seguridad digital.

CATEGORIA DE POLITICA	ACTIVIDADES DE GESTION	PRODUCTO	RESPONSABLE	PERIODICIDAD
	Definir e implementar la política de Seguridad digital, soportado en lineamientos claros acordes a las necesidades de la Institución.	Documento de política seguridad digital	Sistemas - MIPG	ANUAL

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:18/07/2025
		Página 11 de 13

SEGURIDAD DIGITAL	- Brindar capacitación en seguridad de la información y seguridad digital, a los colaboradores	Acta de socialización, registro fotográfico	Sistemas	Semestral
	Implementar mecanismos y herramientas que permitan prevenir, atender, controlar y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.	Guía de proceso dónde se evidencie la prevención de incidentes digitales.	Sistemas	Semestral
	Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e infraestructura implementando estrategias de mejoramiento continuo.	Plan de mejoramiento	Sistemas	Semestral

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
 www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 5 de 13

✓ Garantizar en un grado la disponibilidad, integridad y confidencialidad de la información digital.

✓ Implementar el plan de capacitación y sensibilización con la finalidad de crear una cultura de seguridad institucional por medio de la aplicación de la normatividad vigente y de la adopción de buenas prácticas.

4. NIVEL DE CUMPLIMIENTO

La Política de seguridad digital, será de obligatorio cumplimiento para todos los funcionarios y contratistas que prestan sus servicios a la ESE HOSPITAL SAGRADO CORAZÓN DE JESÚS, independientemente de su tipo de vinculación.

5. APLICABILIDAD

La política de seguridad digital, es una política transversal por lo tanto será aplicable a los todos los servidores de la E.S.E. Hospital Sagrado Corazón de Jesús. La responsabilidad de los servidores públicos y demás colaboradores es llevar a cabo las directrices planteadas en esta política, dando a conocer la aplicación e implementación de lo aquí definido. Es un compromiso y responsabilidad de todos conocer la Política y es deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta.

6. TERMINOS DE REFERENCIA

- **Activo de Información:** Es todo aquello que en la Entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 6 de 13

- ***Carpetas Compartidas:*** Es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- ***CAU:*** Es el único Centro de Atención al Usuario en donde el grupo TIC presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TIC en la ESE Hospital Sagrado Corazón de Jesús
- ***Confidencialidad:*** La información no se pone a disposición ni se revela a individuos, Entidades o procesos no autorizados.
- ***Copias de respaldo:*** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- ***Dato:*** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- ***Disponibilidad:*** Acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, Entidades o procesos autorizados cuando lo requieran.
- ***Drive:*** Sitio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.
- ***Información:*** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- ***Información confidencial o crítica:*** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en la institución
- ***Integridad:*** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 7 de 13

- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
- **OTSI:** Oficina de Tecnología y Sistemas de Información.
- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones

De acuerdo al diagnóstico que se realiza a la política de seguridad digital, se puede evidenciar que se debe priorizar las actividades más importantes para el cumplimiento de los objetivos y metas de la E.S.E.

7. MARCO NORMATIVO

A continuación, se enuncian algunas de las normas que regulan la planificación institucional para asegurar una gestión integral eficiente, eficaz y transparente que evidencie cambios substanciales en el accionar de la entidad hacia la comunidad educativa y fuera de ella generando impacto en el territorio insular. Entre las cuales se encuentran:

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
 www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 8 de 13

- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- **Decreto 454 del 21 de marzo de 2020.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.
- **Decreto 1287 del 24 de septiembre de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Decreto 338 de 2022:** “Por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital”.
- **Directiva Presidencial 03 de 15 de marzo de 2021:** Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.
- **Ley Estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Resolución 500 de 2021:** “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- **Constitución política de Colombia 1991, Artículo 1:** Define a la intimidad y al buen nombre.
- **Decreto 2693 de 2012:** Estrategia de gobierno en línea. Ministerio de tecnologías de la información y las comunicaciones.
- **DECRETO 2364 DE 2012:** Firma electrónica
- **LEY 962 DE 2005.** Simplificación y realización de trámite. Atributos de seguridad en la información electrónica de entidades públicas.

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
 www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 9 de 13

8. POLITICA SEGURIDAD DIGITAL

La presente política tiene como finalidad una adecuada gestión de la información, buscando establecer un marco de confianza en el ejercicio de sus deberes para con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Por medio de la Política de Seguridad digital, tiene como objetivo definir los lineamientos para preservar la integridad, disponibilidad y confidencialidad de la información conforme al cumplimiento de los requisitos legales, estratégicos, operativos, tecnológicos y tácticos, aplicando las buenas prácticas de seguridad de la información digital.

Fortalecer la participación en la mejora de las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso de seguridad digital convocadas por la ESE Hospital sagrado corazón de Jesús.

La ESE Hospital sagrado corazón de Jesús, está comprometida en garantizar el tratamiento de los datos personales, por lo cual se acoge a las disposiciones contenidas en la Ley 1581 de 2012 y la Política de Tratamiento de Datos Personales, que tiene por objetivo establecer los criterios bajo los cuales se recolectan, almacenan, usan, circulan y suprimen los datos personales tratados así como el procedimiento para la garantía de los derechos de los titulares de los datos personales.

La tercera línea de defensa está a cargo de la oficina de control interno, quienes realizan la auditoria de seguimiento a los planes de acción, verificando el cumplimiento de los lineamientos establecidos.

9. IMPLEMENTACIÓN DE LA POLITICA

La implementación de la política por parte de la Empresa Social del Estado Hospital Sagrado corazón de Jesús, se hará a través de la adopción e implementación de lo exigido por el MinTIC quien elaboró el Modelo de Seguridad y Privacidad de la Información – MSPi y define los lineamientos para la implementación de la estrategia de seguridad digital, proteger y darle seguridad a la información, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5)

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 10 de 13

fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información.

Fase: 1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción de la política de seguridad digital. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

Fase 2. Planificación: Determinar las necesidades y objetivos de seguridad digital teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo, para a elaborar el Plan de Seguridad digital.

Fase 3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Fase 4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción de la política de seguridad digital.

Fase 5. Mejoramiento Continuo: Establecer procedimientos para identificar falencias y mejorar el proceso continuo de la política seguridad digital.

CATEGORIA DE POLITICA	ACTIVIDADES DE GESTION	PRODUCTO	RESPONSABLE	PERIODICIDAD
	Definir e implementar la política de Seguridad digital, soportado en lineamientos claros acordes a las necesidades de la Institución.	Documento de política seguridad digital	Sistemas - MIPG	ANUAL

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
 www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 11 de 13

SEGURIDAD DIGITAL	- Brindar capacitación en seguridad de la información y seguridad digital, a los colaboradores	Acta de socialización, registro fotográfico	Sistemas	Semestral
	Implementar mecanismos y herramientas que permitan prevenir, atender, controlar y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.	Guía de proceso dónde se evidencie la prevención de incidentes digitales.	Sistemas	Semestral
	Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e infraestructura implementando estrategias de mejoramiento continuo.	Plan de mejoramiento	Sistemas	Semestral

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 12 de 13

9.1 RESULTADOS ESPERADOS DE LA POLÍTICA

- Fortalecimiento de la Seguridad Digital de la institución.
- Brindar confianza a nuestros usuarios y colaboradores
- Establecer las buenas prácticas que lleven a la confidencialidad, seguridad y disponibilidad de la información digital, que permita minimizar el riesgo de pérdida de datos.
- Desarrollo de las estrategias de la Política de Seguridad Digital buscan contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente el Hospital

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración:
		Página 13 de 13

10. BIBLIOGRAFIA

- <https://gobiernodigital.mintic.gov.co/portal/>
- Como opera Mipg, Función Publica.
<https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>
- <https://revistaseguridad360.com/>

CONTROL DE CAMBIOS

FECHA	DESCRIPCION	VERSIÓN
04-03-2024	Se elabora documento con el fin de establecer la política de seguridad digital en la ESE Hospital sagrado corazón de Jesús, en cumplimiento de la Matriz ITA dando alcance al anexo técnico 2 de la Res. 1519 de 2020	V1

Excelencia y servicio a la comunidad

Dirección: Barrio la Parker vía el Rosal Celular: 3108379335 - 3182528532
 www.hospitalhormiga.gov.co - Email: gerencia@hospitalhormiga.gov.co
 La Hormiga - Valle del Guamuez – Putumayo

	E.S.E HOSPITAL SAGRADO CORAZON DE JESUS NIT 846.000.471 – 5	Código:
		Versión: 1
	POLITICA SEGURIDAD DIGITAL	Fecha Elaboración: 18/07/2025
		Página 12 de 13

9.1 RESULTADOS ESPERADOS DE LA POLÍTICA

- Fortalecimiento de la Seguridad Digital de la institución.
- Brindar confianza a nuestros usuarios y colaboradores
- Establecer las buenas prácticas que lleven a la confidencialidad, seguridad y disponibilidad de la información digital, que permita minimizar el riesgo de pérdida de datos.
- Desarrollo de las estrategias de la Política de Seguridad Digital buscan contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente el Hospital