Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

ESE HOSPITAL SAGRADO CORAZON DE JESUS

2024 -2026

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad.

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

MARCO LEGAL

- ✓ 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).

- ✓ Activo En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- ✓ 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).

- ✓ Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- ✓ Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- ✓ Datos Personales Públicos Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

1. PRESENTACIÓN

Mediante el Plan de Seguridad y Privacidad de la Información de la ESE Hospital Sagrado Corazón de Jesús, tiene como objetivo aplicar los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC basados en los componentes de Gobierno en línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca salvaguardar los datos de los pacientes como bien intangible, garantizando la seguridad de la información.

2. DEFINICIONES

- ✓ **ACTIVOS DE INFORMACIÓN**: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- ✓ **AVISO DE PRIVACIDAD**: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- ✓ **CLASIFICACIÓN DE INFORMACIÓN**: Es la clasificación que se debe dar en función de los requisitos legales, valor, criticidad, y susceptibilidad a divulgación o modificaciones no autorizadas.
- ✓ **INTEGRIDAD**: La información y sus métodos de procesamiento deben ser completos y exactos.
- ✓ **DISPONIBILIDAD**: La información y los servicios deben estar disponibles en el momento que sea requerido.
- ✓ **CONFIDENCIALIDAD**: La información debe ser accesible sólo a aquellas personas autorizadas.
- ✓ **CONTROL**: 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.
- ✓ **DATO PERSONAL**: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.
- ✓ **DATO PÚBLICO**: 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.

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

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.

- ✓ **DATO SEMIPRIVADO**: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- ✓ **DATO PRIVADO**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- ✓ **DATO SENSIBLE**: 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.
- ✓ **INFORMACIÓN CLASIFICADA**: Es aquella información que estando en poder o custodia de un sujeto, 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 de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a los siguientes derechos:
    a. El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado;
    b. El derecho de toda persona a la vida, la salud o la seguridad;
    c. Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011.

  Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable.
  (Artículo 6, literal c y 18 Ley 1712 de 2014).
- ✓ **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 de manera motivada y por escrito, por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. Se podrá negar el acceso a esta información cuando concurra una de las siguientes circunstancias y siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:
    a. La defensa y seguridad nacional;
    b. La seguridad pública;
    c. Las relaciones internacionales;

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

d. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
e. El debido proceso y la igualdad de las partes en los procesos judiciales;
f. La administración efectiva de la justicia;
g. Los derechos de la infancia y la adolescencia;
h. La estabilidad macroeconómica y financiera del país;
i. La salud pública.

Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.
(Artículo 6, literal d y artículo 19 Ley 1712 de 2014).

- ✓ **TRANSFERENCIA**: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país.

3. OBJETIVO

Realizar diferentes actividades para la identificación activos y riesgos de información asociados a los diferentes procesos que la ESE Hospital Sagrado Corazón de Jesús posee dentro del modelo organización, de tal manera que se puedan medir los riegos inherentes y residuales de la entidad.

3.1 OBJETIVOS ESPECIFICOS

- ✓ Crear e implementar las políticas de seguridad y privacidad de la ESE Hospital Sagrado Corazón de Jesús.
- ✓ Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la ESE Hospital Sagrado Corazón de Jesús para tener un Plan de Seguridad y Privacidad de la Información.
- ✓ Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

3. DIAGNOSTICO

Actualmente la ESE HOSPITAL SAGRADO CORAZON DE JESUS cuenta con un protocolo de seguridad de información en la custodia de todos los datos tanto para los pacientes “clientes externos” como también nuestros empelados “clientes internos” de la misma forma la custodia y respaldo de todo el material de apoyo y de trabajo de cada una de las dependencias que cuenta la institución.

4. REPONSABLE

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

- ✓ Gerente
- ✓ Líderes de Procesos
- ✓ Todos los usuarios o funcionarios de la institución.

5. RECURSOS

- ✓ Humano: Gerente, Sub Gerente, Líderes de Proceso, Ingenieros de Sistemas
- ✓ Físico: Infraestructura Tecnológica

6. FORMULACION DEL PLAN

La ESE HOSPITAL SAGRADO CORAZON DE JESUS en su modelo de gestión de calidad tiene incorporado en el proceso de apoyo sistemas de información y la comunicación mecanismos para la seguridad y la privacidad de la información contemplado como contingencia el cual aporta las herramientas necesarias que aportan al presente plan en todo lo relacionado con la seguridad y privacidad.

HERRAMIENTAS DE APOYO

Contamos con varias alternativas de control y autocontrol que aplican a la seguridad y la privacidad de la información entre ellos:

- ✓ Respaldo externo de la institución de la información de la institución (Base de Datos).
- ✓ Herramientas de respaldo automático para la base de datos en el SERVIDOR.
- ✓ Servidor para respaldo de la información de los funcionarios de la institución.

7. ACTIVIDADES

- ✓ Gestión de Activos
- ✓ Política de tratamiento de Datos
- ✓ Custodia de la Información
- ✓ Seguridad física y Ambiental
- ✓ Aspectos de seguridad de la información en la gestión de continuidad de la empresa

Realizar actividades preventivas de respaldo

- ✓ Verificar automatización de los procesos de respaldo para el SERVIDOR.
- ✓ Verificar los procesos de respaldo para la información de los funcionarios.

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

Riesgo	Descripción del Riesgo	Clase o tipo de Riesgo	Causas (Factores Internos o Externos)	Efectos	Tipo de Impacto	Controles Existente	Zona de Riesgo	Acciones	Respon
Software sin licencias y desactualización de las existentes	Que los usuarios instalen software ilegales o las licencias no sean renovadas en el tiempo pertinente	Riesgos de Cumplimiento	1. Desconocimiento de normas relacionadas con derechos de autor 2. Falta de Presupuesto 3. Falta de control en los usuarios y el manejo de Internet.	Sanciones	Impacto Legal	Restricciones de instalación y desinstalación de programas	Alta	1. Realizar visitas a las diferentes dependencias para revisar qué tipo de software está instalado y retirarlo de los equipos. 2. Revisión de fecha de vencimiento de licencias. 3. Montaje de Control específicos que permitan la limitación de Instalación de software no autorizado. 4. Solicitar inclusión en el presupuesto la compra de licencias.	Dependencia de Sistemas y Gerencia.
Copias de Seguridad	custodia y administración de las copias de seguridad	Riesgos Operativos	1. Problemas eléctricos y daño en los equipos de respaldo. 2. Ataque Cibernético. 3. Daño o Pérdida de los equipos de respaldo externos.	Perdida de información alojada en los servidores	Impacto Operativo	Copias de seguridad o Backups hechas diariamente y almacenadas en la nube	Alta	1. Creación de Protocolo de Copias de Seguridad. 2. Realizar copias de seguridad periódicas. 3. Análisis de otras alternativas de custodia.	Dependencia de Sistemas
Daño en la estructura tecnológica	Perdida de conexión a las bases de datos y recuperación de la Información	Riesgos Operativos	1. No cumplimiento del cronograma de mantenimiento Preventivo. 2. Desastres Naturales. 3. Ataques Cibernéticos	Perdida de Información y suspensión de los servicios prestados.	Impacto Operativo	Actualización de Hardware de Servidores y control de ejecución de Mantenimiento Preventivo.	Baja	Inclusión de Nuevos equipos al Cronograma de Mantenimientos	Dependencia de Sistemas
Daño en Bases de Datos	Perdida de Información	Riesgos Operativos	1. Acceso no restringido a los usuarios a los servidores. 2. no existencia de una política de seguridad informática.	Perdida de Información y datos inconsistentes.	Impacto Operativo	Claves de Acceso a la conexión a los servidores.	Alta	1. Restringir acceso al servidor. 2. Conexión Remota con clave restringida.	Dependencia de Sistemas
Daño Eléctrico	Perdida de información	Riesgos Operativos	1. Las UPS Central no está funcionando. 2. Instalar Otra UPS con mejores características 3. Ampliar el Centro de Datos no se puede trabajar allí	Perdida de Información Parcial o Total	Impacto Operativo	Instalación de UPS General	Alta	1. Instalación de UPS y red eléctrica regulada **SOLO** para los equipos de computo	Dependencia de Sistemas y Gerencia.
No hay Antivirus	Perdida de información	Riesgos Operativos	1. Amenazas Cibernéticas	Perdida de Información Parcial o Total	Impacto Operativo	Se está usando el antivirus por defecto de Microsoft Windows Defender	Media	1. Adquisición de un Software de Antivirus Licenciado	Dependencia de Sistemas y Gerencia.

8. IDENTIFICACION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

Calle 12 N 8-99 B. Nazareth, Valencia - Córdoba
314 5609641 esehscj@hotmail.com
www.esehscj.com

9. SEGUIMIENTO E IMPLEMENTACION

Según lo mencionado anteriormente se describe a continuación las etapas que se desarrollaran y los tiempos esperados para alcanzar el presente plan:

- ✓ Revisión y/o Modificación plan de Seguridad y privacidad.
- ✓ Después de la revisión se entrega actas de reunión e informe de avances

10. CRONOGRAMA

Actividades	2024	2025	2026
Verificar protocolos de seguridad	01/03/2024		
Iniciar Plan		01/06/2025	
Realizar seguimiento y mejora		15/09/2025	15/09/2026

ELABORÓ:	REVISÓ:	APROBÓ:
_____	_____	_____
MAURICIO CONEO ROMERO INGENIERO DE SISTEMAS	JHANINA DIAZ VIDAL JEFE DE CALIDAD	ALBERTO VIDAL DIAZ GERENTE