CONTENIDO

1. OBJETIVO 2
2. ALCANCE 3
3. MARCO NORMATIVO 4
4. DIRECTRICES 5
5. MECANISMO DE EVALUACIÓN 12

INTRODUCCIÓN:

La ESE Hospital La María es una institución dedicada a brindar servicios de salud de alta calidad a la comunidad, comprometida con la seguridad y privacidad de la información de sus pacientes. Conscientes de la importancia de un ciclo completo para proteger la información que se maneja en la institución, se ha desarrollado este Manual de Seguridad y Privacidad de la Información, con el fin de establecer las políticas, procedimientos y medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información, y evitar su uso indebido.

En este manual se establecen las políticas y procedimientos que rigen la seguridad y privacidad de la información que se maneja en la ESE Hospital La María, con el fin de cumplir con los requisitos legales y normativos en materia de protección de datos y garantizar la confianza de los pacientes en la institución.

1. OBJETIVO

Establecer las políticas, procedimientos y medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información en la ESE Hospital La María. Además, se busca fomentar la cultura de seguridad de la información en la institución, y concientizar al personal sobre la importancia de proteger la información de los pacientes.

1.1 OBJETIVOS ESPECIFICOS

a. Identificar y evaluar los riesgos a los que está expuesta la información de los pacientes, para establecer medidas de seguridad adecuadas.

b. Definir los roles y responsabilidades de cada uno de los empleados en relación con la seguridad y privacidad de la información.

c. Establecer políticas y procedimientos claros para el manejo de la información en la institución, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

d. Implementar medidas de seguridad técnicas y físicas adecuadas para proteger la información, como el uso de contraseñas seguras, la encriptación de datos sensibles, el control de acceso físico a las instalaciones y un sistema de backups.

e. Fomentar la cultura de seguridad de la información entre los empleados, mediante capacitaciones y sensibilización sobre los riesgos asociados con la información de los pacientes.

f. Involucrar a cada empleado en el papel crucial en la generación de respaldos. Implementaremos pautas flexibles para la periodicidad de respaldos, adaptadas al volumen e importancia asignados en cada etapa del ciclo de la información. El objetivo es garantizar la eficacia de nuestras medidas de seguridad y fomentar la participación activa de todos los miembros de la organización en la protección de la información confidencial, construyendo así un entorno más seguro y robusto.

g. Establecer procedimientos para el manejo de incidentes de seguridad de la información, con el fin de minimizar el impacto y garantizar la continuidad del servicio.

h. Establecer los ciclos de auditorías de seguridad de la información, para evaluar la efectividad de las medidas de seguridad y detectar posibles debilidades en el sistema.

2. ALCANCE

Aplica a todos los empleados, colaboradores y terceros que trabajen con información de pacientes y que tengan acceso a los sistemas de información de la institución. Esto incluye a todos los departamentos, áreas y unidades del Hospital, así como a los proveedores de servicios que manejen información de los pacientes.

Este manual establece las políticas y procedimientos que se deben seguir para garantizar la confidencialidad, integridad y disponibilidad de la información, y para prevenir su uso indebido. Se aborda la protección de la información en todas sus formas, un sistema de respaldo de datos ya sea en formato electrónico o en papel, y en todas las etapas de su ciclo de vida, desde su creación hasta su eliminación.

Además, este manual se enfoca en cumplir con los requisitos legales y normativos en materia de protección de datos, en particular, con la Ley Estatutaria 1581 de 2012, y su decreto reglamentario 1377 de 2013, que establecen las obligaciones de las entidades públicas y privadas en relación con la protección de datos personales.

En resumen, el alcance de este Manual de Seguridad y Privacidad de la Información de la ESE Hospital La María es garantizar la protección de la información de los

pacientes en la institución, a través de políticas y procedimientos claros, medidas de seguridad adecuadas y una cultura de seguridad de la información.

3. MARCO NORMATIVO

El Manual de Seguridad y Privacidad de la Información de la ESE Hospital La María se enmarca en un conjunto de leyes y normativas que tienen como objetivo proteger la información personal de los ciudadanos. A continuación, se describen algunas de las normas más relevantes que son aplicables al manejo de la información de los pacientes en la institución:

a. **Constitución Política de Colombia**: Reconoce el derecho fundamental a la privacidad, el cual incluye la protección de los datos personales.

b. **Ley 1581 de 2012**: Establece el régimen general de protección de datos personales, y regula el manejo de esta información por parte de personas naturales y jurídicas, de naturaleza pública o privada.

c. **Decreto 1377 de 2013**: Reglamenta parcialmente la Ley 1581 de 2012, y establece los requisitos y procedimientos para la protección de datos personales.

d. **Resolución 1995 de 1999**: Establece las normas para el manejo de historias clínicas en Colombia, y regula el acceso a la información médica.

e. **Resolución 1860 de 2018**: Regula el manejo de datos personales en el sector salud, y establece los requisitos para la implementación de medidas de seguridad y privacidad en la información de los pacientes.

Además de estas leyes y normativas, existen otras disposiciones aplicables al manejo de la información en la ESE Hospital La María, como, por ejemplo, los reglamentos internos y las políticas y procedimientos establecidos por la institución para garantizar la protección de la información y la seguridad de los pacientes. Es importante que todos los empleados y colaboradores estén familiarizados con estas normativas y las cumplan de manera rigurosa, para garantizar la protección de los datos personales de los pacientes y el cumplimiento de las obligaciones legales y normativas.

4. DIRECTRICES

Deben ser cumplidas por todos los empleados, colaboradores y terceros que manejen información de la ESE Hospital La María, en aras de garantizar la seguridad y privacidad de la información:

a. **Acceso restringido:** Solo se permitirá el acceso a la información de los pacientes a aquellos empleados o colaboradores que tengan una necesidad legítima de conocerla en el desempeño de sus funciones, y que hayan sido autorizados previamente.

b. **Identificación y autenticación:** Todos los usuarios de los sistemas de información de la institución deben contar con una identificación y una contraseña únicas y seguras, y deberán cambiarlas periódicamente.

c. **Monitoreo y registro:** Se debe llevar un registro de todas las actividades realizadas con la información de los pacientes, incluyendo consultas, modificaciones o eliminaciones, con el fin de detectar y prevenir posibles incidentes de seguridad.

d. **Almacenamiento seguro:** Toda la información de los pacientes debe ser almacenada en lugares seguros, tanto en formato electrónico como en papel, con medidas de protección adecuadas para garantizar su confidencialidad e integridad.

e. **Transmisión segura:** La información de los pacientes solo podrá ser transmitida de manera segura, a través de medios cifrados o seguros, y siempre respetando los requisitos legales y normativos.

f. **Actualización y mantenimiento:** Los sistemas de información y la información de los pacientes deben ser actualizados y mantenidos de manera constante, con el fin de prevenir vulnerabilidades y garantizar su disponibilidad y acceso.

g. **Eliminación segura:** Cuando la información de los pacientes ya no sea necesaria, deberá ser eliminada de manera segura, siguiendo los procedimientos y plazos establecidos por la institución y por la normativa vigente.

h. **Capacitación constante:** Todos los empleados y colaboradores que manejen información de los pacientes deben recibir capacitación constante en materia de seguridad y privacidad de la información, y estar al tanto de los cambios y actualizaciones normativas y tecnológicas.

i. **Información de terceros:** La información de los pacientes solo podrá ser compartida con terceros autorizados y en cumplimiento de los requisitos legales y normativos.

j. **Reporte de incidentes:** Todos los empleados y colaboradores que identifiquen algún incidente de seguridad o privacidad de la información deberán reportarlo de manera inmediata al área encargada de la seguridad de la información, para que se tomen las medidas necesarias de manera oportuna.

k. **Procedimiento de entrega de información:** Se debe entregar toda la información por parte de los empleados, colaboradores y terceros que se desvinculan de la institución o si es solicitado por el líder del proceso. Este procedimiento debe incluir los documentos que son requeridos por el líder del proceso, supervisor o subgerencia, el plazo para la entrega deberá ser en un máximo de 5 días calendario, la forma en que se deben entregar son a discreción del jefe de área, supervisor o subgerente el cual se volverá responsable de la recepción de la información.

l. **Responsabilidades de los líderes de área:** Los líderes de área deben ser los órganos de control encargados de verificar el cumplimiento de esta política. Deben asegurarse de que los empleados, colaboradores y terceros que se vinculan y desvinculan de la institución apliquen las políticas de seguridad y privacidad de la información, además de entregar toda la información que hayan generado durante su vinculación con la institución. Asimismo, deben asegurarse de que la información entregada se maneje de forma segura y se elimine en caso de que no sea necesaria.

m. **Obligación de confidencialidad:** La ESE Hospital La María y sus empleados y colaboradores, incluyendo terceros que tengan acceso a la información confidencial de la institución, se comprometen a mantener la confidencialidad y la privacidad de toda la información que se maneje dentro de la institución.

La información confidencial incluye cualquier información que sea propiedad de la institución, que se maneje en el ejercicio de sus funciones y que no sea de dominio público. Esta información incluye, entre otros, datos personales de los pacientes, información financiera, información administrativa, registros médicos y cualquier otro tipo de información que se considere confidencial.

Las partes se comprometen a no divulgar, transmitir, distribuir, publicar, copiar o utilizar cualquier información confidencial para cualquier fin que no sea el que se establece en el ejercicio de sus funciones dentro de la institución. Las partes se comprometen a no divulgar información confidencial a terceros sin el consentimiento previo y por escrito de la institución.

Las partes se comprometen a proteger la información confidencial y a tomar todas las medidas necesarias para evitar su divulgación, pérdida, alteración, destrucción o uso no autorizado. Las partes también se comprometen a informar inmediatamente a la institución sobre cualquier incidente de seguridad o posible violación de la privacidad de la información.

La obligación de confidencialidad de las partes continuará incluso después de la terminación de su relación con la institución. Las partes reconocen que cualquier incumplimiento de esta cláusula puede ocasionar daños y perjuicios a la institución y se comprometen a indemnizar y eximir de responsabilidad a la institución por cualquier daño o perjuicio que se genere por su incumplimiento.

La presente cláusula de confidencialidad será vinculante para las partes y sus respectivos sucesores y cesionarios.

Esta obligación debe estar respaldada por un compromiso de confidencialidad que se firme al momento de la desvinculación.

n. **Capacitación:** Es importante que los empleados, colaboradores y terceros que generan información y que se desvinculan de la institución reciban capacitación sobre la importancia de la entrega de información y la obligación de confidencialidad esta estará a cargo del personal jurídico de la ESE Hospital La María.

o. **Medidas de seguridad:** Se deben establecer medidas de seguridad para garantizar que la información entregada se maneje de forma segura y se elimine en caso de que no sea necesaria. Estas medidas pueden incluir el uso de software de borrado seguro de datos, la encriptación de los datos y el monitoreo de las actividades de los usuarios.

p. **Esquema de controles de seguridad**

Nº	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Gestión de usuarios y privilegios	Establecer políticas de acceso basadas en roles y privilegios. Implementar la autenticación de dos factores para usuarios con acceso a información crítica.	Equipo de Seguridad de la Información.
2	Implementar tecnologías de encriptación	La implementación de encriptación constituye un pilar fundamental en la estrategia de seguridad de la información, salvaguardando la confidencialidad de datos tanto almacenados como transmitidos. En reposo, la encriptación se aplica mediante tecnologías como el encriptado de disco completo y la protección de bases de datos individuales, asegurando que, en caso de acceso no autorizado, la información permanezca ilegible sin la clave correspondiente. En tránsito, protocolos seguros y	Equipo de Seguridad de la Información.

		conexiones VPN se utilizan para prevenir la interceptación de datos durante la transmisión. La gestión segura de claves criptográficas es esencial, involucrando la generación, almacenamiento, rotación y revocación adecuada de claves. Este enfoque global fortalece la postura de seguridad, garantizando que incluso en escenarios adversos, la confidencialidad de la información se mantenga intacta.	
3	Implementar herramientas de monitoreo en tiempo real.	Mediante el sistema integral de monitoreo y detección de intrusiones para fortalecer la postura de seguridad de la red. Esta actividad implica la configuración de sistemas avanzados de monitoreo en tiempo real, centrados en la identificación de patrones de actividad anómala o maliciosa en la red. A través de la supervisión constante de registros de eventos y el análisis de anomalías	Equipo de Seguridad de la Información.
4	Actualizaciones y Parches de Seguridad	Esta actividad implica la aplicación sistemática de actualizaciones proporcionadas por los desarrolladores para abordar vulnerabilidades recién identificadas. Mantener un programa de gestión de parches eficiente no solo significa incorporar nuevas características y mejoras de rendimiento, sino, y quizás más crucialmente, cerrar posibles brechas de seguridad que	Equipo de Seguridad de la Información.

		podrían ser explotadas por amenazas cibernéticas	
5	Creación y prueba regular de respaldos.	**Servidores:** • **Proceso:** • Realizar respaldos completos de servidores de manera regular (al menos semanalmente). • Almacenar respaldos en ubicaciones seguras, considerando sistemas locales y servidores remotos. • Ejecutar pruebas periódicas de recuperación (recomendación: al menos mensualmente) para verificar la efectividad de los respaldos. **2. Bases de Datos:** • **Proceso:** • Aplicar estrategias específicas de respaldo para garantizar la coherencia y la integridad de los datos almacenados en bases de datos esenciales, utilizando el sistema de mantenimiento de base de datos, aplicando sistema de compresión de datos. • Almacenar respaldos en ubicaciones seguras y ejecutar pruebas	Equipo de Seguridad de la Información. Lideres De Área o Proceso

		regulares de recuperación (al menos trimestralmente) para verificar la integridad de los datos. **3. Aplicaciones ERP:** • **Proceso:** • Respaldar aplicaciones ERP críticas junto con sus configuraciones para facilitar una recuperación sin inconvenientes. • Almacenar respaldos de aplicaciones ERP en ubicaciones seguras y realizar pruebas regulares de recuperación (recomendación: al menos trimestralmente). **4. Registros de Usuarios:** • **Proceso:** • El usuario es responsable de identificar y notificar al área de tecnología sobre los recursos críticos que desea respaldar, especificando la naturaleza temporal o permanente de dichos datos. • El usuario deberá ejecutar los respaldos de manera autónoma, utilizando las herramientas y	

		procesos proporcionados por el área de tecnología para garantizar la integridad de la información. • La notificación al área de tecnología debe incluir detalles claros sobre la frecuencia y la urgencia de los respaldos, así como cualquier cambio en los requisitos de respaldo. • La responsabilidad directa de la ejecución y el mantenimiento de los respaldos recae en el usuario, quien deberá seguir las directrices proporcionadas por el área de tecnología. • Los usuarios deben estar al tanto de las políticas de protección de datos y notificar al área de tecnología sobre cualquier cambio o irregularidades sobre la custodia y manejo de la información.	

5. MECANISMO DE EVALUACIÓN

Auditorías internas: La ESE Hospital La María debe llevar a cabo auditorías periódicas para evaluar el cumplimiento del manual de seguridad y privacidad de la información por parte de sus empleados y colaboradores. Las auditorías deben ser

realizadas por personal capacitado e independiente que no tenga relación con las áreas evaluadas.

Evaluaciones de riesgos: La ESE Hospital La María debe llevar a cabo evaluaciones periódicas de riesgos para identificar los riesgos potenciales para la seguridad y privacidad de la información, y establecer medidas de mitigación.

Encuestas de satisfacción: La ESE Hospital La María puede realizar encuestas de satisfacción a sus pacientes y usuarios para evaluar su percepción sobre la protección de su información personal y médica.

Revisiones periódicas: La ESE Hospital La María debe llevar a cabo revisiones periódicas del manual de seguridad y privacidad de la información para evaluar su efectividad y actualizarlo en caso de ser necesario.

Capacitaciones: La ESE Hospital La María debe proporcionar capacitación continua a sus empleados y colaboradores sobre el manual de seguridad y privacidad de la información, para asegurarse de que comprendan sus obligaciones y responsabilidades.

Pruebas de penetración: La ESE Hospital La María puede llevar a cabo pruebas de penetración para evaluar la seguridad de sus sistemas de información y redes.

Revisiones de terceros: La ESE Hospital La María puede contratar a terceros para llevar a cabo revisiones independientes del manual de seguridad y privacidad de la información y de los controles implementados.

ELABORÓ	REVISO	APROBÓ
Sergio Sebastian Muñoz Mejia Líder de TIC	Noralba Castaño Puerta Líder Calidad	Ramon Antonio Lema Hurtado Subgerente Administrativo