Hospital Regional
de Sogamoso E.S.E.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Resolución 455 del 31 de diciembre de 2024

"Por medio de la cual se establece el compromiso de la alta dirección por la política de privacidad y seguridad de la información del Hospital Regional de Sogamoso E.S.E."

El Suscrito Gerente del Hospital Regional de Sogamoso E.S.E. en uso de sus atribuciones legales y,

CONSIDERANDO QUE,

Que la Constitución Política de Colombia en su artículo 15 consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Que mediante decreto 1011 de 2006, se establece el Sistema Obligatorio de garantía de Calidad de la atención en salud del Sistema general de Seguridad Social en Salud, que define las norma, requisitos, mecanismos y procesos desarrollados en el sector salud para generar, mantener y mejorar la calidad de los servicios de salud en el país.

Que la ley 1266 de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones, en el artículo 4 establece "los principios de la administración de los datos: principio de veracidad o calidad de los registros o datos, principio de finalidad, principio de circulación restringida, principio de temporalidad de la información, principio de interpretación integral de derechos constitucionales, principio de seguridad y principio de confidencialidad.

Que la ley 1273 de 2009 por medio de la cual se modifica el Código penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Que la ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales en los principios rectores artículo 4 literal g, establece el principio de seguridad "La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o

acceso no autorizado o fraudulento" y el literal h, establece el principio de confidencialidad "Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma".

Que el Decreto 1377 de 2013 por el cual se reglamenta parcialmente la ley 1581 de 2012, derogado parcialmente por el Decreto 1081 de 2015, determina en el numeral 3 del artículo 3 " 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".

Que la norma técnica NTC-ISO/IEC 27001:2013, tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. (SGSI). Requisitos, determina en el numeral 4 el "Sistema de gestión de la seguridad de la información".

Que la ley 1712 de 2014 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, establece en el artículo 3 "otros principios de la transparencia y acceso a la información pública" en la interpretación del derecho de acceso a la información se deberá adoptar un criterio de razonabilidad y proporcionalidad, así como aplicar los siguientes principios: principio de transparencia, principio de buena fe, principio de facilitación, principio de no discriminación, principio de gratuidad, principio de celeridad, principio de eficacia, principio de la calidad de la información, principio de la divulgación proactiva de la información y principio de la divulgación proactiva de la información

Que la resolución 2082 y Decreto 903 del 2014, establece los estándares de acreditación dirigidos hacia la mejora de los resultados de la atención en salud, centrados en el usuario, que van más allá de la verificación de la existencia de estructura o de la documentación de procesos.

Que la resolución 5095 de 2018 del Ministerio de Salud y Protección Social, por la cual se adopta el "Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia versión 3.1" establece en los Estándar 143 y 146 criterios de seguridad y confidencialidad de la información.

Resolución 3100 de 2019, Ministerio de Salud y Protección Social, Por la cual se definen los procedimientos y condiciones de inscripción de los prestadores de servicios de salud

y de habilitación de los servicios de salud y se adopta el Manual de Inscripción de Prestadores y Habilitación de Servicios de Salud.

Que el Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG) versión 4 en el numeral 3.2.1.2 Política Gobierno Digital literal habilitadores transversales: Seguridad de la información " : Busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos".

Que el Hospital Regional de Sogamoso E.S.E. para el Plan de Desarrollo 2024-2027 "Un Hospital en el que puedes confiar establece la meta de modernización institucional en la cual se establece optimizar la infraestructura física y fortalecer la capacidad tecnológica e informática del hospital, asegurando la disponibilidad de equipos modernos y sistemas eficientes, con el fin de mejorar y agilizar los procesos administrativos y asistenciales.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: COMPROMISO: El Hospital Regional de Sogamoso E.S.E. se compromete con la implementación de un sistema de gestión de seguridad de la información que busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión.

ARTICULO SEGUNDO: LINEAS ESTRATEGICAS: EL Hospital Regional de Sogamoso E.S.E. establece como líneas estratégicas para la implementación y despliegue de la política privacidad y seguridad de la información las siguientes líneas:

Línea estratégica 1: Acceso y uso de la información

- **Acceso restringido**: Solo personal autorizado puede acceder a archivos de gestión, centrales e históricos, así como a las historias clínicas, bajo condiciones específicas.
- **Uso adecuado**: Sistemas de información destinados exclusivamente para asuntos del hospital; uso personal prohibido.
- **Protección de historias clínicas**: Se prohíbe modificar la información diligenciada y el uso de comandos de copiar y pegar.

Línea estratégica 2: Administración de contraseñas

- **Seguridad de contraseñas**: Contraseñas de uso personal, no deben ser reveladas ni escritas. Reportar cualquier uso no autorizado.
- **Gestión de cuentas**: Controles para identificar responsables de la creación y modificaciones de cuentas.
- **Estándares de contraseñas**: Contraseñas deben cumplir con requisitos de complejidad según la criticidad de la información.

Línea estratégica 3: Uso de cuentas para acceso a recursos tecnológicos

- **Roles y funciones**: Definición clara para reducir usos no autorizados. Revisión semestral por el líder de gestión de recursos informáticos.

Línea estratégica 4: Acceso a la red por terceros

- **Uso exclusivo de equipos hospitalarios**: Acceso a la red solo para equipos autorizados.
- **Control de acceso**: Acceso a información solo con autorización formal y análisis previo. Trazabilidad de acciones garantizada.

Línea estratégica 5: Seguridad y confidencialidad

- **Integridad de archivos**: Verificación de condiciones físicas y técnicas de archivos clínicos.
- **Uso profesional del correo electrónico**: Precaución con destinatarios colectivos y cumplimiento de leyes de derechos de autor.
- **Notificación de riesgos**: Informar cualquier evento que comprometa la confidencialidad y seguridad de la información.
- **Aceptación de reglamentación**: Usuarios deben aceptar formalmente las políticas de acceso y tratamiento de información.
- **Control de acceso de terceros**: Restricciones para acceso de terceros hasta que se implementen controles apropiados y se firmen acuerdos.
- **Documentación formal**: Manuales y procedimientos para proteger la información compartida con terceros

Línea estratégica 6: Gestión de medios removibles

- **Restricción de conexión no autorizada**: Prohibición del uso de dispositivos personales no institucionales sin autorización.
- **Protección física y control**: Los medios removibles que contienen información institucional deben ser controlados y físicamente protegidos.
- **Identificación y autorización**: Cada medio removible debe estar identificado según su contenido y el tránsito de estos medios debe ser autorizado.

Línea estratégica 7: Conservación y prevención del deterioro de la información

- **Sistema Integrado de Conservación**: Incluye actividades como diagnóstico integral, prevención de desastres y control ambiental.
- **Copias de seguridad**: Realización de copias de seguridad diarias, semanales y mensuales.
- **Protección de información crítica**: Medidas como bloqueo de equipos y uso de contraseñas.
- **Precauciones con documentos**: No reutilizar papel sensible y retirar documentos impresos inmediatamente.

Línea estratégica 8: Control documental (físico – digital)

- **Confidencialidad en gestión documental**: Responsabilidad de mantener la confidencialidad y seguridad de documentos físicos y digitales.
- **Organización de archivos digitales**: Uso de estructuras de nombres para garantizar la organización.
- **Procedimientos operativos**: Instrucciones para manejo de errores y recuperación de sistemas.

Línea estratégica 9: Control de cambios operativos

- **Justificación y documentación de cambios**: Todos los cambios a la infraestructura deben ser justificados, documentados y sometidos a pruebas.
- **Análisis de riesgos**: Evaluación de riesgos de implementación y no implementación de cambios.

Línea estratégica 10: Manejo de la información financiera

- **Bloqueo automático de equipos**: Control del tiempo de inactividad.
- **Limitación de privilegios de usuario**: Reducir riesgos asociados con la instalación de software no autorizado.
- **Medidas de seguridad adicionales**: Restricciones en el uso de software no necesario, ejecución de archivos y acceso remoto.
- **Mantenimiento y actualización**: Solo personal autorizado puede realizar estas tareas.
- **Navegador único y actualizado**: Uso de un navegador configurado para máxima seguridad en transacciones financieras
- eras.
- **Redes inalámbricas seguras**: Aislamiento de redes WIFI para invitados.
- **Autenticación y control**: Uso de perfiles de autorización y notificaciones en línea para transacciones

ARTICULO TERCERO: OBJETIVO: Establecer e implementar la política a través del programa privacidad y seguridad de la información del Hospital Regional de Sogamoso

E.S.E. y las sedes adscritas, estableciendo las políticas, procedimientos e instructivos en materia de seguridad de la información, Fortaleciendo la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Hospital Regional de Sogamoso E.S.E.

ARTICULO CUARTO: ALCANCE. Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Hospital Regional de Sogamoso E.S.E. y la ciudadanía en general.

ARTICULO QUINTO: RESPONSABLES DE LA IMPLEMENTACIÓN: La alta dirección y el equipo gestión de la información del Hospital Regional de Sogamoso E.S.E quien evalúa y promueve la política de privacidad y seguridad de la información.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI del Hospital Regional de Sogamoso E.S.E.:

- Hospital Regional de Sogamoso E.S.E. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- Hospital Regional de Sogamoso E.S.E. protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- Hospital Regional de Sogamoso E.S.E. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido
  a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Hospital Regional de Sogamoso E.S.E. protegerá su información de las amenazas originadas por parte del personal.
- Hospital Regional de Sogamoso E.S.E. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Hospital Regional de Sogamoso controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Hospital Regional de Sogamoso E.S.E. implementará control de acceso a la información, sistemas y recursos de red.
- Hospital Regional de Sogamoso garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Hospital Regional de Sogamoso E.S.E. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- Hospital Regional de Sogamoso E.S.E. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- Hospital Regional de Sogamoso E.S.E. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de seguridad y privacidad de la información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

ARTÍCULO SEXTO: VIGENCIA: La presente resolución rige a partir de la fecha de su expedición y deroga las demás disposiciones que le sean contrarias.

Dada en Sogamoso, a los treinta y un (31) días del mes de diciembre (12) del año dos mil veinticuatro (2024).

COMUNÍQUESE Y CÚMPLASE

En constancia firma,

LIFAN MAURICIO CAMACHO MOLANO
Gerente
Hospital Regional de Sogamoso E.S.E.

Proyecto y elaboró: Yeiler Eduardo Bernal Gutierrez, Profesional Especializado Lider TI
Revisó: Jenith Lorena López Rodríguez, Líder Gestión de Calidad
Andrea Milena Benítez Malaver, Líder Desarrollo Organizacional
Erika Natalia Sánchez Medina, Subgerente Administrativa y Financiera