Hospital Regional de Sogamoso
Empresa Social del Estado
Nit 891855039-9

POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

Resolución 358 del 19 de octubre de 2021

"Por medio de la cual se adopta la POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN del HOSPITAL REGIONAL DE SOGAMOSO E.S.E."

La Suscrita 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 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 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 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.

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 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".

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: ADOPCIÓN: Adoptar la Política de Confidencialidad y Seguridad de la Información en el Hospital Regional de Sogamoso E.S.E. y las Unidades Básicas de Atención (UBA).

ARTÍCULO SEGUNDO: OBJETIVO.

La política de Confidencialidad y Seguridad de la Información en el Hospital Regional de Sogamoso E.S.E, tendrá como objetivo:

Garantizar de manera constante que el 100% de los datos personales, historia clínica, datos que revelen el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual de los usuarios, manejados en todos los procesos, trámites, servicios, sistemas de información e infraestructura del Hospital Regional de Sogamoso E.S.E, se utilicen de forma segura y confidencial, certificando la disponibilidad, integridad, confidencialidad y privacidad de la información relacionada con los funcionarios y usuarios.

ARTÍCULO TERCERO: ALCANCE.

La Política de Confidencialidad y Seguridad de la Información es transversal a todos los procesos e involucra a todos los niveles de la institución y deberá ser implementada por los colaboradores, personal en formación de la institución, independientemente de su modalidad de contratación o vinculación.

ARTÍCULO CUARTO: RESPONSABLES.

Es responsabilidad de todos los niveles de la entidad, colaboradores, funcionarios, contratistas, empresas subcontratadas, usuarios sin excepción alguna y demás personas que realicen alguna actividad laboral en el Hospital Regional de Sogamoso E.S.E. y las Unidades Básicas de Atención (UBA) cumplir la Política de confidencialidad y Seguridad de la Información.

ARTÍCULO QUINTO: DEFINICIONES.

El Hospital Regional de Sogamoso E.S.E, adopta la terminología para la Política de Confidencialidad y Seguridad de la Información así:

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, etc.) que tenga valor para la organización.

Amenaza informática: La aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Autorización: Consentimiento que, de manera previa, expresa e informada emite el Titular de algún dato personal para que un tercero lleve a cabo el Tratamiento de sus datos personales.

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 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.

Base de Datos Personal: Es todo conjunto organizado de datos personales que es objeto de Tratamiento.

Ciclo de Vida Dato Personal: Hace referencia al proceso de recolección, almacenamiento, clasificación, análisis, uso, transferencia, retención y destrucción del dato personal.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos 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, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos Sensibles: Se entiende por datos sensibles aquellos datos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, bien sea porque revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, organizaciones de derechos humanos, que promuevan 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.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Habeas data: Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Principios para el Tratamiento de Datos: Son las reglas fundamentales, de orden legal y/o jurisprudencial, que inspiran y orientan el Tratamiento de datos personales, a partir de los cuales se determinan acciones y criterios para dar solución a la posible colisión entre los derechos a la intimidad, Habeas Data y protección de los datos personales, y el derecho a la información.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la Base de Datos y/o el Tratamiento de los datos.

Seguridad de la Información.
La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Sistema de Gestión de Seguridad de la Información (SGSI)

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Titular: Es la persona física cuyos datos sean objeto de Tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión de estos.

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 de Colombia.

Transmisión: Tratamiento de los datos personales que implica la comunicación de los mismos dentro y fuera de Colombia cuando tenga por objeto la realización de un Tratamiento por parte del encargado por cuenta del responsable.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Tecnología de la Información: Se refiere al hardware y software operados por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del hospital, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Usuario: Corresponde a un cliente, un potencial cliente o un usuario que solicita los servicios del Hospital Regional de Sogamoso E.S.E.

ARTÍCULO SEXTO: DEFÍNASE LOS SIGUIENTES COMPONENTES DE LA POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

- **De acceso y uso de la información**

a) Solo tendrán acceso al archivo (de gestión, central e histórico) las personas debidamente autorizadas para tal fin, las demás se entienden "personal no autorizado".
b) En todo caso solo tendrán acceso a la Historia Clínica: El usuario, el equipo de salud; las autoridades judiciales de salud en los casos previstos en la Ley; los autorizados por el paciente o apoderados del mismo; las aseguradoras cuando presenten la autorización firmada por el paciente; los padres, familiares o tutelantes cuando se trate de pacientes incapacitados mentalmente o menores de edad o cuando su revelación es útil al tratamiento.
c) Los sistemas de información de la Institución son primordialmente para uso de asuntos relacionados con la misma.
d) El uso personal para acceder, descargar, transmitir, distribuir o almacenar información para fines distintos a los legalmente contemplados por la entidad, está totalmente prohibido.
e) La historia clínica se debe guardar automáticamente y se debe garantizar que la información diligenciada no pueda ser modificada y no se puede hacer uso de los comandos copiar y pegar.
f) Queda prohibido el uso de software no licenciado en la entidad.

- **De administración de contraseñas**

Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que sean asignados:

a) Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
b) Las contraseñas no deberán ser reveladas.
c) Las contraseñas no se deberán escribir en ningún medio.
d) Es deber de cualquier funcionario y contratista reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, y debe catalogarse como un incidente de seguridad.
e) La asignación de toda cuenta de acceso a un componente electrónico de procesamiento de información debe cumplir con controles que permitan identificar los responsables de las actividades de solicitud, aprobación, creación, modificación, inactivación o eliminación autorizada de la cuenta de acceso, así como el mantenimiento de la veracidad y trazabilidad de las actividades realizadas para la asignación de la cuenta de acceso.
f) Toda acción realizada empleando la cuenta de acceso debe ser registrada mediante controles que permitan mantener la trazabilidad de las mismas.
g) Toda cuenta de acceso empleará como mínimo una contraseña como mecanismo de autenticación seguro.

h) Toda contraseña para cuenta de acceso debe cumplir con los estándares de contraseña segura, dependiendo de la criticidad de la información. El estándar básico debe incluir mínimo 8 caracteres, una mayúscula, letras minúsculas y un número, para sistemas de información con información crítica, se debe incluir la obligatoriedad de un símbolo especial (* % ~ §, etc.)
i) Toda cuenta de acceso es personal e intransferible.
j) Toda cuenta de acceso debe ser asignada formalmente a una persona quién responderá por su uso y acciones realizadas con la misma en el componente electrónico de procesamiento de información o con la información del componente de procesamiento de información.
k) Toda cuenta de acceso que no cuente con un responsable en un término de tiempo de un mes de manera temporal o definitiva debe ser inhabilitada para evitar su uso por parte de otros usuarios o componentes electrónicos de procesamiento de información que no estén formalmente autorizados y permanecerá inhabilitada hasta tanto no esté disponible el responsable de la cuenta de acceso o se decida su inactivación definitiva.

- **De uso de cuentas para acceso a recursos tecnológicos**

a) Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos, para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.
b) La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada semestralmente por el líder de gestión de recursos informáticos, con el fin de mantener actualizada dicha información y acorde con la realidad de cada uno de los procesos del hospital.

- **De acceso a la red por terceros**

a) La red de área local (LAN) es de uso exclusivo de los equipos del hospital.
b) Todo funcionario, proceso o sistema de información que realice actividades para el Hospital deberá tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas.
c) Todo acceso a la información deberá ser autorizado formalmente por el área responsable de la información. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.
d) El acceso a la información del hospital debe estar sujeto a controles que garanticen la trazabilidad de las acciones realizadas sobre la misma, considerando la identificación de la persona, proceso o sistema que realiza el acceso, acciones realizadas, instante de tiempo en que se realizan las acciones y ubicación desde la cual se realiza el acceso a la misma.

- **De seguridad y confidencialidad**

a) El Hospital Regional de Sogamoso E.S.E debe asegurar las condiciones de los archivos de historias clínicas verificando que se garantice la integridad física y técnica sin adulteración o alteración de la información. De igual forma se hace extensible para los demás sistemas de archivo. Las acciones de estos usuarios están vinculadas con el secreto profesional.
b) Todos los instrumentos descriptivos de los archivos clínicos diseñados e implementados por la Institución, son de uso exclusivo de la misma.
c) El correo electrónico debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los destinatarios colectivos. Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.
d) Cualquier evento que implique un riesgo para la preservación de la confidencialidad, seguridad, integridad, disponibilidad, autenticidad o trazabilidad de la información debe ser notificado al líder de proceso de gestión de recursos informáticos.
e) El acceso a la información obliga a la aceptación formal por parte del usuario o el responsable del componente electrónico de procesamiento de información de la reglamentación de acceso y tratamiento de la información que defina las leyes de Colombia, acuerdos internacionales suscritos por Colombia, normas del sector, políticas, estándares o cualquier tipo de control establecido para la protección o tratamiento de la información.
f) En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica y que deban desarrollarse dentro del Hospital, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar para el acceso a información sensible.
g) En ningún caso se otorgará acceso a terceros a la información sensible, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.
h) Deben existir manuales, procedimientos y formatos formalmente aprobados por el Hospital para proteger la información o servicios que se compartan con terceros. Los mecanismos administrativos formales definirán claramente el tipo de información, su clasificación, acuerdos para uso y protección de la información. Los terceros deben aceptar y cumplir la política de seguridad de la información del hospital.

- **De gestión de medios removibles**

a) Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica del Hospital de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras

fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

b) Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.
c) La entidad definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas, estás serán definidas por la subgerencia administrativa y financiera y la subgerencia científica, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.
d) Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene.
e) El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

- **Conservación y prevención del deterioro de la información**

a) El Sistema Integrado de Conservación será el eje fundamental que garantice la preservación de la información física, en donde se deben realizar las siguientes actividades: Diagnóstico integral; Sensibilización y toma de conciencia; Prevención y atención de desastres; Inspección y mantenimiento de instalaciones; Monitoreo y control de condiciones ambientales; Limpieza de áreas y documentos; Control de plagas; Apoyo a la producción documental y manejo de correspondencia; Almacenamiento, Re almacenamiento y empaste/ encuadernación (Determinación de Espacios y áreas locativas, determinación de mobiliario y equipo, determinación de Unidades de conservación y almacenamiento).
b) Se realizarán copias de seguridad diarias, semanales y mensuales por parte del área de sistemas. Dichas copias reposaran en los servidores de la Institución. Cada usuario de sistemas de cómputo es responsable de realizar las copias de seguridad cuando lo considere necesario.
c) En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
d) Los usuarios deberán bloquear su equipo cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.
e) Todos los equipos de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por el hospital, el cual se activará automáticamente después del tiempo de inactividad definido por el líder de gestión de recursos informáticos, y se podrá desbloquear únicamente con la contraseña del usuario.
f) Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
g) No se deberá reutilizar papel que contenga información sensible.
h) Los usuarios no deberán almacenar en los equipos documentos, accesos directos a los mismos o a sistemas de información sensibles.

i) Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.
j) Los registros médicos no pueden dejarse o archivarse en sitios físicos donde no esté restringido el acceso a visitantes o personal no autorizado.

- **De control documental (físico – digital)**

a) Todos los servidores públicos son responsables de mantener la confidencialidad y seguridad de la Gestión Documental institucional generada físicamente, digitalmente o a partir del Correo Electrónico, de acuerdo con las disposiciones vigentes.
b) Los Usuarios de cada uno de los Sistemas de información son responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas en el sistema.
c) Para fortalecer el archivo de información digital, se recomienda utilizar la siguiente estructura (FECHA_NOMBRE DEL ARCHIVO) de tal manera que se garantice la organización y búsqueda de dicha información.
d) Los procedimientos operativos deben contener instrucciones para el manejo de errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los hubiere lugar.

- **De control de cambios operativos**

a) Todos los cambios a la infraestructura de información y tecnología deben estar plenamente justificados.
b) Todos los cambios deben ser formalmente documentados.
c) Todos los cambios deben incluir un análisis de los riesgos de su implementación y de su no implementación.
d) Todos los cambios deben ser sometidos a algún mecanismo de prueba que permita verificar si su planificación está completa antes de su ejecución.

- **De manejo de la información financiera**

La entidad deberá asegurarse de lo siguiente:

a) Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil. (2 minutos).
b) Limitar los privilegios de las cuentas de usuario utilizadas para realizar transacciones financieras en los equipos, a efecto de reducir el riesgo de que

con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.

c) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.
d) Efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas.
e) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil, sea realizada únicamente por los funcionarios del proceso de gestión de recursos informáticos.
f) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones.
g) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada.
h) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).
i) Restringir el software de acceso remoto al equipo que pueda ofrecer o tener preinstalado el Sistema Operativo del respectivo equipo o terminal.
j) Procurar tener instalado un solo navegador, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las instituciones financieras con las que tenga relación, con mejores mecanismos de seguridad posibles debidamente configurados y el cual deberá estar permanentemente actualizado a efecto de garantizar la disposición de mejoras o correcciones a su funcionamiento.
k) Restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o terminal. Esto con el objeto de evitar que, de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.
l) Deberá evitarse realizar transacciones financieras desde dispositivos móviles o conexiones a redes inalámbricas de terceros no confiables.
m) Si la entidad cuenta con una red inalámbrica (WIFI) para invitados, esta deberá estar totalmente aislada y segmentada de las redes LAN de la entidad.
n) Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones. Particularmente, definir perfiles de autorización de transacciones, utilizar la preinscripción de beneficiarios, parametrizar montos y horarios para la realización de operaciones y realizar la inscripción para recibir notificaciones en línea.

ARTÍCULO SÉPTIMO: COMPROMISO

El Hospital Regional de Sogamoso E.S.E. se compromete a desarrollar en todos sus procesos, trámites, servicios, sistemas de información e infraestructura, un correcto uso y tratamiento de los datos personales, historia clínica y datos sensibles contenidos en las bases de datos, evitando el acceso no autorizado a terceros que puedan conocer o vulnerar, modificar, divulgar y/o destruir la información que allí reposa, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.

ARTÍCULO OCTAVO: AVISO DE PRIVACIDAD DE PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y Decretos reglamentarios, el presente Aviso de Privacidad tiene como objeto informar al Titular de los datos personales (en adelante "el usuario del Hospital") sobre el tratamiento al cual serán sometidos los datos almacenados en las bases de datos del Hospital Regional de Sogamoso E.S.E. (en adelante "el Hospital") e informar si estos estarán sujetos a transmisión y/o transferencia a terceras entidades.

La Política de Tratamiento de Datos Personales, Resolución 033 del 23 de enero del 2019 del Hospital Regional de Sogamoso E.S.E. se podrá consultar a través de la página web www.hospitalsogamoso.gov.co.

El Hospital Regional de Sogamoso E.S.E. está domiciliado en la ciudad de Sogamoso departamento Boyacá, en la Calle 8 a No 11 – 43 , Barrio la Castellana, y recibe notificaciones con respecto a tratamiento de datos personales en el correo electrónico atencionalusuario@hospitalsogamoso.gov.co correo y dirección electrónica a la que podrá remitirse por escrito si desea presentar consultas, peticiones o reclamos que se traten sobre protección de datos personales.

El Hospital será el responsable de canalizar todas las solicitudes que se remitan a este correo electrónico por el tratamiento de los datos directamente recolectados o por el tratamiento dado por los encargados de los datos personales de los usuarios.

Las condiciones del tratamiento son las siguientes:

En desarrollo de su actividad, el Hospital podrá realizar las siguientes actividades relacionadas con el manejo de datos personales:

1. Efectuar las gestiones pertinentes para el desarrollo de cada una de las etapas para atención en el Hospital Regional de Sogamoso E.S.E., respecto de cualquiera de los servicios ofrecidos o que solicite el usuario, respecto de cualquier relación

contractual subyacente que tenga con ella, así como dar cumplimiento a la ley en Colombia y las órdenes de autoridades judiciales o administrativas.

2. Gestionar trámites (solicitudes, quejas, reclamos), realizar análisis de riesgo, efectuar encuestas de satisfacción respecto servicios prestados por el Hospital Regional de Sogamoso E.S.E., así como sus aliados comerciales.
3. Usar la información en procesos de investigación científica para la búsqueda de estrategias en la promoción y prevención de patologías de cualquier índole.
4. Dar a conocer, transferir y/o trasmitir mis datos personales, a terceros a consecuencia de solicitudes de los entes de control o las normas emitidas en el proceso legal de acuerdo a la ley de Colombia.
5. Realizar a través de cualquier medio en forma directa o a través de terceros, programación y publicidad e información correspondiente al portafolio de servicio del Hospital Regional de Sogamoso E.S.E. y su objeto social.
6. Para el envío y recepción de información o material publicitario de acuerdo a los requerimientos de las funciones demandadas y sostenibilidad de los servicios del Hospital Regional de Sogamoso E.S.E.
7. Controlar y prevenir el fraude en cualquiera de sus modalidades.

La política de tratamiento de datos personales, así como los cambios sustanciales que se produzcan en ella, se podrán consultar a través de la página web **www.hospitalsogamoso.gov.co**.

Es de carácter facultativo suministrar información que trate sobre Datos Sensibles, entendidos como aquellos que afectan la intimidad o generen algún tipo de discriminación, o sobre menores de edad.

ARTÍCULO NOVENO: PRINCIPIOS PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

Los principios que se indican en el presente artículo son los lineamientos que serán respetados por el Hospital, en los procesos de recolección, almacenamiento, uso, administración de los datos personales:

Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al Titular. De esta manera, el Tratamiento de datos personales al interior de El Hospital se efectuará: en el marco de las relaciones jurídicas contractuales que se celebre con sus distintos grupos de interés; en el marco de la ley cuando deba cumplirse un Tratamiento por mandato legal y; acorde con la finalidad previamente expresada al Titular del dato en aquellos casos en que el Tratamiento se realice de manera puntual.

Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular, o expresado mediante actos inequívocos. Los datos

personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: En el Tratamiento debe garantizarse el derecho del usuario del Hospital Regional de Sogamoso ESE a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley 1581 de 2012 y la Constitución y demás normas que las complementen. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en la internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.

Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento, 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.

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.

ARTÍCULO DÉCIMO: SENSIBILIZACIÓN Y CAPACITACIÓN

Considerando que el público objetivo es todo el personal del hospital y usuarios, el líder de gestión de recursos informáticos realizará las siguientes estrategias:

- Comunicación interna: En forma directa y personal con los trabajadores y usuarios del Hospital Regional de Sogamoso E.S.E. a través de charlas, talleres con apoyo de elementos impresos o audiovisuales orientados a sensibilizar a los participantes
- Comunicación externa: A través de la página web de la entidad en el link de

transparencia y acceso a la información pública y videos institucionales publicados en las redes sociales de la entidad.

ARTÍCULO DÉCIMO PRIMERO: IMPLEMENTACIÓN DE LA POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN.

El Hospital Regional de Sogamoso E.S.E. y las Unidades Básicas de Atención (UBA) establece los lineamientos para la implementación designando como responsables de la ejecución de los componentes de confidencialidad y seguridad de la información al proceso de gestión de recursos informáticos y todos los líderes de la institución, quienes, mediante campañas pedagógicas, socialización y sensibilización darán a conocer los lineamientos de implementación de la presente política, informando al personal y usuarios de la entidad.

ARTÍCULO DÉCIMO SEGUNDO: INTEGRACIÓN CON OTRAS POLÍTICAS

La Política de confidencial y seguridad de la información se articula con la política de tratamiento de datos personales en el Hospital Regional de Sogamoso E.S.E. por cuanto la misma busca establecer y comunicar los lineamientos aplicables al tratamiento de datos personales recolectados, tratados y/o registrados en las bases de datos en desarrollo del objeto social de la entidad.

ARTÍCULO DÉCIMO TERCERO: RECURSOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

En la planeación presupuestal del hospital, se incluirán los recursos requeridos para garantizar la implementación de la presente Política, asegurando el apoyo financiero, físico, tecnológico y de Talento Humano para el logro del objetivo aquí planteado.

ARTÍCULO DÉCIMO CUARTO: INDICADORES QUE MIDEN LA POLÍTICA

- % de implementación de la política en todos los procesos de la entidad.
- % backup realizados de la información de la entidad.
- % de adherencia de roles definidos para garantizar la seguridad y confidencialidad de la información.

ARTÍCULO DÉCIMO QUINTO: DOCUMENTOS DE REFERENCIA

- Guías Modelo de Seguridad y Privacidad de la Información. Seguridad y

Privacidad de la información. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC).

- Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia. Versión 3.1. Ministerio de Salud y Protección Social de Colombia.

ARTICULO DÉCIMO SEXTO: VIGENCIA Y DEROGATORIAS. La presente Resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en Sogamoso, a los 19 (diecinueve) días del mes de octubre del año 2021.

En constancia firma,

SHEYLA FANORY CAICEDO RINCÓN
Gerente

Elaboró: Fredy González – Líder de proceso Gestión de recursos informáticos
Lina María Espinel Aguirre – Profesional especializado en mejoramiento continuo

Revisó: Oscar Darío Soler Morales – Asesor Planeación Institucional
Iris Adriana Mojica Carvajal – Asesor de Programas Especiales y Gestión de Calidad
Diego Fernando Fuquén Fonseca – Subgerente Administrativo y Financiero