RESOLUCION No. 0162

(17 JUN 2021)

"Por medio de la cual se adopta la política institucional privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá y se dictan otras disposiciones"

EL GERENTE DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN RAFAEL DE FUSAGASUGÁ,

En uso de las atribuciones que le confieren la Ley, los Estatutos y.

CONSIDERANDO:

Que la Constitución de Colombia en su Artículo 15, se establece 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 los bancos de datos y en archivos de entidades públicas y privadas".*

Que la Ley 1266 de 2008 del Congreso de la República, *"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".*

Que la Ley 1273 de 2009 del Congreso de la República, *"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 1712 de 2014 del Congreso de la República, *"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".*

Que la Ley 594 DE 2000, *"Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".*

Que la resolución 0287 del 28 de diciembre de 2018 *"Por medio de la cual se adopta la política de gestión documental de la E.S.E Hospital San Rafael de Fusagasugá y de determinan otras disposiciones".*

Norma Técnica NTC-ISO/IEC Colombiana 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos

Que la Resolución 066 de 2018 de la E.S.E. Hospital San Rafael de Fusagasugá, *"Por medio de la cual se crea el Comité de Gestión y Desempeño en la E.S.E. Hospital San Rafael de Fusagasugá, en cumplimiento del Decreto 1499 del 11 de septiembre de 2017". En su Artículo primero, objeto "Crear el comité de Gestión y Desempeño de la E.S.E. Hospital San Rafael de Fusagasugá, el cual sustituirá los demás comités que tengan relación con el Modelo Integrado de Planeación y Gestión y que no sean obligatorios por mandato legal".*

En mérito de lo anteriormente expuesto,

RESUELVE

ARTÍCULO PRIMERO. OBJETO: Adoptar la política institucional de privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá.

"La E.S.E. Hospital San Rafael De Fusagasugá tiene como propósito salvaguardar los recursos de información de la entidad y la tecnología utilizada para su procesamiento, en cuanto a posibles amenazas, internas o externas, dando cumplimiento a los pilares de la seguridad de la información: confidencialidad, integridad, disponibilidad, y autenticidad de la información mediante la gestión de riesgos y establecimiento de controles".

RESOLUCION No. 0162

(17 JUN 2021)

"Por medio de la cual se adopta la política institucional privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá y se dictan otras disposiciones"

ARTÍCULO SEGUNDO. OBJETIVOS: La política institucional de privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá establece los siguientes objetivos.

2.1. OBJETIVO GENERAL: Definir procedimientos adecuados para la administración y buen manejo de la información institucional tanto física como digital garantizando interoperabilidad con todas las áreas que intervienen en los procesos y uso de la información.

2.2. OBJETIVOS ESPECÍFICOS: Se determinan los siguientes objetivos específicos de la política de privacidad y seguridad de la información:

2.2.1. Establecer los lineamientos básicos que regirán el uso la infraestructura y que brinden seguridad lógica y física a los servicios y sistemas.

2.2.2. Realizar la gestión integral de los riesgos que ponga en vulnerabilidad la información, estableciendo controles necesarios para el manejo de la información y recursos tecnológicos haciendo énfasis en fortalecer la cultura de privacidad y seguridad de la información en los funcionarios, contratistas aprendices, practicantes y terceros.

ARTÍCULO TERCERO. DEFINICIONES: En la implementación, aplicación y seguimiento de la política institucional de privacidad y seguridad de la E.S.E. Hospital San Rafael de Fusagasugá se deberán tener en cuenta las siguientes definiciones:

3.1. 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).

3.2. 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).

3.3. ACTIVO DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

3.4. 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

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

3.6. AUDITORIA: Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

3.7. BASES DE DATOS PERSONALES: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

3.8. CIBERSEGURIDAD: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

3.9. CONTROL DE ACCESO: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria, Una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

3.10. DATOS ABIERTOS: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

3.11. DATOS PERSONALES: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

3.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

3.13. INFORMACIÓN PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

3.14 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 por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

3.15. PLAN DE TRATAMIENTO DE RIESGOS: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

3.16. PRIVACIDAD: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

3.17. RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

3.18. SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

3.19. 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. (ISO/IEC 27000).

3.20. VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

ARTÍCULO CUARTO. PRIVACIDAD Y TRATAMIENTO DE LA INFORMACIÓN: Los funcionarios, contratistas aprendices, o practicantes pueden tener acceso únicamente a la información necesaria y usada exclusivamente para la ejecución de las funciones y/o actividades contractuales

ARTÍCULO QUINTO: POLÍTICA DE SEGURIDAD EN RECURSOS HUMANOS: Gestión del talento humano deberá informar a los funcionarios en capacitaciones de inducción la responsabilidad que se debe tener frente a la privacidad y seguridad de la información, esto estableciéndolo como un control en los riegos de robo, fraude o uso indebido de la información.

ARTÍCULO SEXTO. GESTIÓN DE ACTIVOS: La E.S.E Hospital San Rafael de Fusagasugá tendrá identificado, clasificado y hará buen uso de los activos de la información, teniendo:

6.1. INVENTARIO DE ACTIVOS: Identificados, clasificados y controlados garantizando la integridad en caso de materialización de riesgos.

6.2. ARCHIVOS DE GESTIÓN: Se debe garantizar la integridad, confidencialidad y disponibilidad de la información.

6.3. CLASIFICACIÓN DE LA INFORMACIÓN: Deberá estar definida conforme a la ley 1712 "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.", Ley 594 DE 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones" y resolución 0287 "por medio

de la cual se adopta la política de gestión documental de la E.S.E Hospital San Rafael de Fusagasugá y de determinan otras disposiciones".

ARTÍCULO SÉPTIMO. CONDICIONES GENERALES DE USO DE EQUIPOS Y/O SERVICIOS TECNOLÓGICOS: Los usuarios de la red y equipos de cómputo del Hospital San Rafael deberán solicitar apoyo u orientación al sub. Proceso de Sistemas ante dudas específicas en el manejo de equipo de cómputo, acceso a la información de los servidores internos y manejo de datos.

En el sub. Proceso de Sistemas los equipos de cómputo, red de datos y demás servicios tecnológicos podrán ser operados por personal de área, administrativo y/o personal previamente autorizado por los responsables de los equipos, en ninguna circunstancia deberán ser operados por personal ajeno a la E.S.E.

Las actividades realizadas en los equipos de cómputo, la red de datos deberán acoplarse a los programas y proyectos administrativos y operativos del Hospital y no para fines personales u ociosos; Los equipos de cómputo cuentan con los programas necesarios para las actividades de administración, investigación y capacitación. Está prohibido el uso, almacenaje, copiado y reproducción de software sin uso de licencia. Algunos usos aceptables de los recursos de cómputo y red de datos contemplan:

a. La investigación apoyada en el uso de recursos de software.

b. Presentaciones, talleres, congresos y seminarios virtuales y en general todas las actividades que promuevan la cultura informática entre la población del Hospital.

c. Realización de cursos internos para capacitación de acuerdo a los requerimientos de cada una de las Unidades Funcionales y/o usuarios del Hospital (Programados por las áreas responsables).

d. Actividades de gestión y administración que requiera el uso de medios electrónicos y sistemas distribuidos.

Los usuarios deberán tener bien definidas las actividades que van a realizar con los equipos de cómputo y red de datos con el fin de lograr un buen desempeño y optimización de los recursos de cómputo.

Si los funcionarios o contratistas del Hospital San Rafael deben hacer uso de equipos ajenos al Hospital estos deberán tener software licenciado y antivirus así un ingeniero del subproceso de sistemas puede dar el aval para que el equipo pueda ser vinculado en la red del Hospital.

ARTÍCULO OCTAVO. ASIGNACIÓN DE USUARIOS Y CLAVES DE ACCESO.: La creación y administración de las contraseñas de los equipos de cómputo, red de datos, sistemas de información, Plataforma de aprendizaje Moodle y correo electrónico es responsabilidad del líder del sub proceso de sistemas y su equipo de trabajo.

La asignación de usuarios y contraseñas para los sistemas de información se realizará, previa autorización de la subgerencia científica, administrativa o comunitaria, enviada al correo electrónico sistemas@hospitaldefusagasuga.gov.co.

Después de que se asigne el usuario y contraseña en los sistemas de información o Plataforma Moodle el usuario deberá cambiarlo en su próximo inicio de sesión, Para realizar el cambio de contraseña debe incluir mínimo una letra mayúscula, un número y un carácter especial.

ARTICULO NOVENO. COPIAS SEGURIDAD: Desde el sub. Proceso de Sistemas se realizan y administran las copias de seguridad de los sistemas de información, adicional se realiza la administración de la NAS donde se encuentra almacenada información de consulta y trabajo de los procesos y sub procesos de la E.S.E Hospital San Rafael.

RESOLUCION No. 0162
(17 JUN 2021)

"Por medio de la cual se adopta la política institucional privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá y se dictan otras disposiciones"

ARTÍCULO DECIMO. CORREO ELECTRONICO: El correo electrónico Institucional se usa exclusivamente para enviar y recibir información institucional, y unos de los propósitos fundamentales es contribuir al uso eficiente y ahorro de papel.

Por medio del correo electrónico no deberá ser enviada información de carácter reservada, no se podrá hacer envió de correo masivos.

Los mensajes sospechosos tanto en su contenido (archivos adjuntos con extensiones .exe, .bak, .pif .bat, .prg) como en su remitente debe ser reportado en el sub proceso de sistemas dado que en su contenido puede tener virus.

No es permitido enviar o reenviar información de la E.S.E Hospital San Rafael a través del correo electrónico diferente a lo que se encuentre del de las funciones u obligaciones de la relación contractual.

ARTÍCULO DECIMO PRIMERO. OTROS LINEAMIENTOS DE USO DE EQUIPOS Y/O SERVICIOS TECNOLÓGICOS: Es imperativo seguir los demás lineamientos están estipulados en El Plan de Seguridad y Privacidad de Información el cual fue aprobado por el comité de Gerencia el 1 de marzo de 2021 el cual hace parte integral de la presente resolución.

ARTÍCULO DECIMO SEGUNDO. SEGUIMIENTO: En la implementación, aplicación y seguimiento de la política institucional de privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá se deberá hacer seguimiento mediante los siguientes aspectos:

9.1. SOCIALIZACIÓN: Se debe realizar al cierre de cada vigencia en el comité institucional de gestión y desempeño, presentación de los avances en cuanto al cumplimiento de las estrategias establecidas para su respectiva implementación, aplicación y seguimiento en cuanto al despliegue, apropiación y operación de la política de privacidad y seguridad de la información.

9.2. RESPONSABILIDAD: La aplicabilidad de la política de privacidad y seguridad de la información de la E.S.E. Hospital San Rafael de Fusagasugá será responsabilidad de la Gerencia, quien a su vez determina como responsable al líder del sub proceso de sistemas.

ARTÍCULO DECIMO TERCERO. ALCANCE: La política de privacidad y seguridad de la información aplica donde la E.S.E. Hospital San Rafael tenga precedencia o desarrolle sus actividades y se realice recolección, procesamiento y almacenamiento de información, y es aplicable a todos y cada uno de los servicios de la E.S.E Hospital San Rafael de Fusagasugá en su sede central, puestos y centros de salud.

ARTÍCULO DECIMO CUARTO. VIGENCIA: La presente resolución a rige a partir de la fecha de expedición y deroga todas las normas que le sean contrarias.

PUBLIQUESE Y CÚMPLASE

ANDRÉS MAURICIO GONZÁLEZ CAYCEDO
Gerente

Elaboro: Filanderson García Gómez - Líder subproceso sistemas.
Diana Mabel Padilla - Profesional subproceso sistemas.
Revisó: Julián Nieto Beltrán - Profesional apoyo planeación.
Jairo Bobadilla Montenegro - Profesional proceso planeación.
Katherin Medellin -Contratista proceso jurídica.
Aprobó: Isidro Alberto González Rodríguez - Subgerente administrativo.