Hospital San Rafael de Fusagasugá

"Hospital humano, hospital comprometido"

2021

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMAS

E.S.E. HOSPITAL SAN RAFAEL DE FUSAGASUGÁ

27/01/2021

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:
SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS SAS
Sistemas

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN RAFAEL DE FUSAGASUGÁ
GESTIÓN DE APOYO
GESTIÓN DE RECURSOS FÍSICOS
AÑO 2021

Aprobación: 27-ENE-2021

TABLA DE CONTENIDO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

Mediante la implementación del plan de seguridad y privacidad de la información se pretende establecer los lineamientos que son base fundamental para apoyar la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo mitigar riesgos para la información.

La E.S.E. Hospital San Rafael de Fusagasugá trabaja en el fortalecimiento de la seguridad de la información, con el fin de fortalecer la información como un activo importante garantizándole protección y privacidad tanto a ciudadanos, funcionarios y en general a la entidad.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Mejorar las buenas prácticas de gestión de la seguridad y privacidad de la información aplicables para la E.S.E. Hospital San Rafael de Fusagasugá.

2.2. OBJETIVOS ESPECIFICOS

- Establecer un plan de comunicación que promueva las mejores prácticas de seguridad de la información en la institución.
- Fortalecer los niveles de seguridad de la información al interior de la entidad.
- Fomentar actividades que permitan mitigar el impacto en cuanto a incidentes con la información encaminada a la seguridad digital.
- Robustecer la transparencia de la gestión pública a nivel institucional.
- Alinear actividades del plan de seguridad de la información con la NTC/IEC ISO 27001:2013.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales.
- Alinear el plan estratégico institucional y el plan estratégico de tecnologías de la información y de las comunicaciones.

3. ALCANCE

El plan de seguridad y privacidad de la información contempla todas las acciones y mecanismos institucionales para garantizar la privacidad y seguridad de la información y aplica para la E.S.E. Hospital San Rafael de Fusagasugá en su sede central, sedes adscritas, centros y puestos de salud, los cuales manejen, información institucional obtenida de la prestación de servicios de salud.

4. CONTENIDO

4.1. NORMATIVIDAD

- DECRETO 612 DE 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".
- NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 tecnología de la información. Técnicas de seguridad Sistemas de gestión de la seguridad de la información (SGSI).
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".
- 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".

4.2. DEFINICIONES

ACCESO A LA INFORMACIÓN PÚBLICA: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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

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.

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.

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

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.

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

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).

CIBERESPACIO: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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.

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).

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

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

DATOS PERSONALES PRIVADOS: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

DATOS PERSONALES MIXTOS: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

DATOS PERSONALES SENSIBLES: 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. (Decreto 1377 de 2013, art 3).

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).

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).

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)

LEY DE HABEAS DATA: Se refiere a la Ley Estatutaria 1266 de 2008.

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA: Se refiere a la Ley Estatutaria 1712 de 2014.

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).

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.

REGISTRO NACIONAL DE BASES DE DATOS: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

RESPONSABLE DEL TRATAMIENTO DE DATOS: 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. (Ley 1581 de 2012, art 3).

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).

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

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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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).

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

4.3. RESPONSABLES

Las responsabilidades para la gestión de plan de seguridad y privacidad de la información de la E.S.E. Hospital San Rafael De Fusagasugá, estarán a cargo de las siguientes áreas:

- Subgerencia administrativa.
- Calidad.
- Planeación.
- Oficina de sistemas.
- Gestión documental.
- Comunicaciones.

4.4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

"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".

La aplicación y cumplimiento de esta política es extensiva a todos los funcionarios, consultores, contratistas, o terceros que accedan a los equipos del hospital, con las respectivas autorizaciones los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que los trabajadores del hospital.

El incumplimiento de la política por negligencia o casualidad hará que la E.S.E. Hospital San Rafael de Fusagasugá, tome las medidas correspondientes, tales como acciones disciplinarias, cesación del contrato de prestación de servicios, acciones legales, reclamo de compensación por daños, etc.

4.4.1. LÍNEAS DE ACCIÓN FÍSICAS Y LÓGICAS

Con el propósito de coordinar la seguridad física y lógica a la infraestructura y datos del sistema de información utilizado por la E.S.E. Hospital San Rafael de Fusagasugá, Dinámica Gerencial Hospitalaria se establecen los siguientes lineamientos a tener en cuenta.

Esta línea de acción está orientada a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) brindando a los funcionarios pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida.

4.4.2. USO, INSTALACIÓN Y MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

La estructura y uso de la red de datos, equipo de conectividad, equipo y áreas de cómputo de la oficina de sistemas de la E.S.E. Hospital San Rafael de Fusagasugá están establecidos bajo el control de una serie de lineamientos que se han venido aplicando para optimizar los procesos de mejoramiento del área de sistemas.

Esta política se ha ido adoptando en cada proceso del hospital donde se hace necesaria la utilización de elementos de cómputo (computadores e impresoras) contribuyendo a una cultura, para el cuidado y adecuado funcionamiento de cada uno de estos equipos.

CONDICIONES GENERALES DE USO

Los usuarios de la red y equipo de cómputo de la E.S.E. Hospital San Rafael de Fusagasugá deberán solicitar apoyo u orientación a la oficina 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 la oficina de sistemas los equipos de cómputo y de la red de datos podrán ser operados por el personal de área, administrativo y/o personal previamente autorizado por los responsables de los equipos, bajo ninguna circunstancia deberán ser operados por personal ajenas a la E.S.E.

Las actividades realizadas en los equipos de cómputo de la red de datos de oficina de sistemas (laboratorios de cómputo, equipos de cómputo para facturación, capacitación y red de datos) deberán acoplarse a los programas y proyectos administrativos 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 el consentimiento por escrito del propietario de los derechos de autor.

Algunos usos aceptables de los recursos de cómputo y red de datos de la oficina de sistemas contemplan:

- La investigación apoyada en el uso de recursos de software.
- Presentaciones, talleres, congresos y seminarios virtuales y en general todas las actividades que promuevan la cultura informática entre la población del hospital.
- 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).
- 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 de la oficina de sistemas, con el fin de lograr un buen desempeño y optimización de los recursos de cómputo del área de sistemas.

RESTRICCIONES Y OBLIGACIONES DE LOS USUARIOS

Todos los usuarios deberán respetar la integridad de los equipos y las instalaciones de cómputo de la oficina de sistemas de la E.S.E. Hospital San Rafael de Fusagasugá, además de la confidencialidad y los derechos individuales de los demás cumpliendo los siguientes ítems:

- Está prohibido fumar, consumir alimentos y/o bebidas en sitios donde se encuentre ubicadas los equipos de cómputo (computadores e impresoras), así como introducir cualquier tipo de arma o estupefaciente, es obligación de los usuarios mantener limpias las áreas donde se encuentren equipos, depositando la basura en los botes destinados para este fin.
- Evitando conectar y/o desconectar componentes de hardware de los equipos de cómputo, ante cualquier falla de los equipos es necesario reportarla a los responsables del área técnica de sistemas para que solucionen el desperfecto.
- No se permite la instalación de cualquier tipo de software sin la autorización de la oficina de sistemas y sin licencia.
- Absteniéndose de consultar material inapropiado, obsceno, pornográfico, de violencia explícita, indecente, ilegal o cualquier otro tipo de material que pudiera ofender a los usuarios de espacios de cómputo comunes. Se hará seguimiento a aquellos usuarios que incumplan esta directriz. Su omisión será reportada a la oficina de control interno.
- No se permite la ejecución de sistemas de mensajería como MSN Messenger, Yahoo Messenger u otros. Su omisión será reportada a la oficina de control interno.
- Absteniéndose de realizar actividades ociosas (juegos, chat, descargar archivos mp3, mp4, videos, imágenes) o ejecución de software desde páginas de Internet y otras actividades que saturen el ancho de banda de la red interna de la E.S.E. Hospital San Rafael de Fusagasugá; bajo ninguna circunstancia la infraestructura de cómputo deberá ser utilizada para lanzar ataques a otros equipos conectados en red.
- No se permite la modificación de configuración de:
  - Conexiones de Red.
  - Pantalla.
  - Sonido.
  - Hora y fecha del sistema.

- Firewall de Windows.
- Cuentas de Usuario.

- Los computadores estarán ubicados en los escritorios o puestos de trabajo teniendo en cuenta las normas emitidas por salud ocupacional buscando siempre el bienestar del personal.

INSTALACIÓN DE EQUIPOS DE COMPUTO

- Todo equipo de cómputo, que esté o sea conectado a la red o aquel que en forma autónoma se tenga debe de sujetarse a las normas técnicas y procedimientos de instalación, tales como conexión a red eléctrica regulada (si se cuenta en el área de trabajo), polo a tierra, utilización de estabilizadores y multi tomas, etc.
- La oficina de sistemas deberá tener un registro de todos los equipos de cómputo propiedad del hospital este registro incluirá el responsable, ubicación, placa de activos fijos (si la tiene) o número de serie y software instalado.
- El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, su acceso que la oficina de sistemas tiene establecido en sus políticas.
- El jefe del proceso de propiedad planta y equipo deberá ordenar a su grupo de colaboradores se cumpla con las normas de instalación de red eléctrica y cableado estructurado cuando se requiera la actualización, reubicación, reasignación de puntos de red y todo aquello que implique movimientos.
- Los equipos de cómputo solo serán entregados por el personal técnico de Sistema con un acta de entrega en donde conste las características del equipo, su estado, accesorios, software instalado y políticas de uso.
- La protección física de los equipos corresponde a quienes en un principio se les asigna y corresponde notificar los movimientos en caso de que existan a la oficina de sistemas quien autorizara o realizara dicho movimiento al nuevo lugar de trabajo y actualizara en la base de datos la ubicación del equipo.

MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

- Corresponde al personal técnico de la oficina de sistemas la realización del mantenimiento preventivo y correctivo de los equipos propios, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar.
- Corresponde a la oficina de sistemas conocer las listas de las personas que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

ACTUALIZACIÓN DE EQUIPO DE CÓMPUTO

- Corresponde al personal técnico de la oficina de sistemas realizar la actualización de los equipos propios en lo referente al hardware, y la actualización de todos los equipos de cómputo del hospital en lo que a software se refiere una vez estudiada la necesidad del usuario.
- Por ningún motivo se autorizará a personal diferente al personal técnico de la oficina de sistemas del hospital o personal técnico de la empresa de renta de equipos a realizar actualizaciones de hardware o software a cualquier equipo del hospital.
- Los equipos de cómputo del hospital tendrán como mínimo el siguiente software básico, el cual debe contar con las licencias de fábrica ej. Sistema operativo, suite ofimática, antivirus, correo institucional.
- El área de sistemas debe velar porque todo el software instalado en los equipos tanto propios como rentados se encuentre licenciado, el software que no esté autorizado, ni se encuentre licenciado debe ser removido de los equipos de cómputo por personal del área de sistemas.

REUBICACIÓN DE EQUIPOS DE CÓMPUTO

- La reubicación de equipo de cómputo se realizará previa solicitud y/o autorización del líder o coordinador del proceso respectivo, al área de sistemas y solo se realizará con autorización del líder de la oficina de sistema por personal técnico del área o por personal del departamento de mantenimiento. Se deberá diligenciar el documento de traslado de equipos entre dependencias establecido por la oficina de activos fijos.

- Todo equipo de cómputo reubicado será actualizado en la base de datos del personal técnico del área de sistemas y se dejará constancia de quien lo solicito y quien lo autorizo, con el fin de tener control sobre la ubicación de los equipos.

SOFTWARE

La E.S.E. Hospital San Rafael de Fusagasugá es una Empresa Social de Estado al servicio del público y caracterizando por su prestigio y trayectoria por ello no se comparte desde ningún punto de vista la ilegalidad ni la piratería, por lo tanto:

- Todo Software que sea instalado en servidores, estaciones de trabajo o equipos de cómputo debe estar debidamente licenciado.
- Solo el personal técnico de la oficina de sistemas podrá realizar instalación de software en las estaciones de trabajo o equipos de cómputo, previa verificación de la licencia, este personal podrá instalar por necesidades del servicio software catalogado con versiones de software libre.
- Por ningún motivo se permitirá que personal ajeno a esta dependencia baje o instale de internet software, archivos de video o música de cualquier tipo incluso si se trata de versiones libres o de demostración.
- No se permite la ejecución de sistemas de mensajería como MSN Messenger, Yazoo Messenger, Facebook Messenger, WhatsApp web entre otros.

USO DE LA RED

- El personal de usuarios deberá abstenerse de realizar actividades ociosas (juegos, chat, descarga y reproducción de archivos divx, mpeg, software, páginas de videos en streaming) y otras actividades que saturen el ancho de banda de la red interna del hospital.
- Bajo ninguna circunstancia la infraestructura de cómputo deberá ser utilizada para lanzar ataques a otros equipos conectados en red u a otras redes.
- Todos los computadores de la red estarán sujetas a la política establecida en la plataforma del antivirus institucional, por ningún motivo se podrán instalar aplicaciones que vulneren de cualquier manera la seguridad de los equipos de computo

MODIFICACIONES AL SERVICIO Y/O EQUIPOS TECNOLÓGICOS

Se cancelará el acceso temporal o permanentemente a los usuarios que hagan uso inadecuado de las instalaciones y equipos de cómputo en espacios comunes, y las modificaciones a los servicios y reanudación de accesos a los mismos serán aplicadas por el personal administrativo de estos espacios.

Estas políticas serán socializadas en todo el Hospital y serán de obligatorio cumplimiento, su omisión será informada a la oficina de control interno disciplinario

ACCESO AL ÁREA DE SISTEMAS

- El centro de datos de la entidad es un área restringida y por tal motivo solo podrá ingresar funcionarios del área o personal autorizado en compañía de un funcionario de la oficina de sistemas.
- El acceso al área de servidores es restringido, la misma permanecerá cerrada; solo el líder del área de sistemas o personal autorizado por el mismo podrán ingresar, para lo cual se debe firmar un formato de ingreso con hora de entrada, hora de salida y motivo.
- La oficina de sistemas deberá contar con rejas en las ventanas y puertas de acceso con chapas de seguridad y el acceso solo deberán ser manejadas por el personal de esta dependencia.

ADMINISTRACIÓN Y MONITOREO DE SERVIDORES

- La administración de los servidores debe realizarse únicamente por el personal aprobado por el profesional del proceso de sistemas.
- Para las plataformas institucionales debe existir un único usuario con privilegios de administrador que será usada y administrada por el profesional del proceso de sistemas.

- La administración y manipulación de los equipos de cómputo que se encuentran en el área de servidores donde residen los sistemas de información solo serán responsabilidad del personal de la oficina de sistema, por tal razón ninguna persona ajena a esta dependencia podrá por ningún motivo manipular estos equipos, ni permanecer en el área restringida donde se encuentran los servidores.
- Todos los equipos de cómputo como computadores de escritorio, computadores portátiles y servidores contaran con antivirus que permitan realzar protección de los mismos de ataques y amenazas cibernéticos internos o externos, con políticas de acuerdo a rol desempeñado en la entidad.

ASIGNACIÓN DE USUARIOS Y CLAVES DE ACCESO

- La creación y administración de las contraseñas de equipos de cómputo de la entidad es responsabilidad del líder de la oficina de sistemas y su equipo de trabajo, dichas contraseñas se asignan por medio del active directory implementado en la entidad.
- La asignación de usuarios y contraseñas para los usuarios que usan el sistema de información Dinámica Gerencial Hospitalaria lo realizara exclusivamente el personal de la oficina de sistemas, previa autorización de la subgerencia científica, administrativa o comunitaria, enviada al correo electrónico sistemas@hospitaldefusagasuga.gov.co.
- La nomenclatura de los usuarios del sistema de información Dinámica Gerencial Hospitalaria corresponderá a número de cedula. La contraseña por será el mismo número de cedula, pero 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.
- Se deberá instruir a los clientes internos (usuarios del sistema de información) en el momento de su entrega sobre el uso y manejo apropiado que le deberán dar a su usuario y contraseña, recalcarles que uso del usuario es personal e intransferible y por ende la responsabilidad solo recaerá sobre el dueño del mismo, la clave de acceso solo la deberá conocer el interesado, en caso de ser necesario este podrá solicitar al administrador del sistema el cambio en cualquier momento.

COPIAS DE SEGURIDAD

- Es responsabilidad del administrador del sistema de información responder por la integridad de la información y por el óptimo funcionamiento del sistema de información, para ello se realizarán backup o copias de seguridad de la siguiente manera:
  - Programación del JOP en el motor de base de datos SQL Server
  - Programar la generación diaria de una copia de seguridad
  - Copia del archivo generado y se entregara una a sub gerencia administrativa.
- Para las copias de seguridad de la información que se encuentra en las estaciones de trabajo se designara en un servidor espacio en el disco duro con capacidad suficiente para alojar la información de los usuarios de la entidad, en este servidor existe una carpeta para cada estación de trabajo, la carpeta se denominara con el nombre del equipo de cómputo.
- El área de sistemas realizará las copias de seguridad de los equipos de cómputo del hospital, lo cual será informado a través del correo interno Institucional. Para tal fin en la fecha programada un técnico del área de sistemas se dirigirá al área donde está ubicado el equipo de cómputo y generará el respaldo de la información, la cual será guardada en un servidor de copias de seguridad. El técnico de sistemas debe registrar en la planilla de soporte de copias de seguridad tamaño inicial de la copia y el tamaño final de la misma la cual debe ser firmada por el usuario del equipo de cómputo con el fin de evidenciar la realización de la actividad. Se realizará respaldo de los siguientes tipos de archivos: Excel, Word, Power Point, Access, archivos PDF, archivos CSV, archivos TXT en versiones existentes en el hospital, y correos internos y externos.

CORREO ELECTRÓNICO INSTITUCIONAL

RESPONSABILIDAD

- El líder de cada área puede tener acceso a internet debiendo ser justificado el motivo por lo cual es necesaria su asignación. Como responsable debe mantener la confidencialidad de su contraseña y de su nombre de cuenta; además, será el único responsable de todas y cada una de las actividades relacionadas con la misma.
- Es importante mencionar que la información transmitida mediante este servicio es responsabilidad única y exclusiva de cada usuario.

CAPACIDAD DE ALMACENAMIENTO Y DURACIÓN DE LA CUENTA

- La cantidad de espacio de almacenamiento de correo electrónico en los servidores por usuario está limitada a 30Gb por cuenta. Algunos mensajes de correo electrónico pueden no ser admitidos debido a restricciones de espacio.

CONDUCTA

- Como condición al uso del servicio, el usuario garantiza a la oficina de sistemas que no utilizará el mismo para fines ilícitos o prohibidos en los presentes términos y condiciones.
- El usuario se comprometerá a usar el Servicio únicamente para enviar y recibir mensajes con fines contractuales, como entes de control, revistas médicas, bancos y demás de uso necesario por las obligaciones como Empresa Social del Estado. Se prohíbe expresamente cualquier uso personal o comercial no autorizado.
- El usuario se comprometerá a cumplir con toda la normativa local, estatal, nacional e internacional aplicable y es único responsable de todos los actos u omisiones que sucedan en relación con su cuenta o contraseña, incluido el contenido de sus transmisiones, pero sin limitarse a ello, el usuario acepta abstenerse de:
  - Usar el servicio en relación con mensajes no deseados, correos molestos (spam) u otros mensajes duplicativos o no solicitados (comerciales o de otro tipo).
  - Difamar, insultar, acosar, amenazar o infringir de cualquier otra forma los derechos de terceros (tales como el derecho a la intimidad o a la propia imagen).
  - Publicar, distribuir o divulgar cualquier información o material inapropiado, obsceno, indecente o ilegal.
  - Recopilar o de cualquier otro modo recabar información sobre terceros, incluidas sus direcciones de correo electrónico, sin su consentimiento.
  - Transmitir o cargar archivos que contengan virus, "caballos de troya", gusanos u otros programas perjudiciales o nocivos.
  - Interferir o interrumpir redes conectadas con el servicio o infringir las normas, directivas o procedimientos de dichas redes.
  - Intentar obtener acceso de forma no autorizada al Servicio, a otras cuentas, a sistemas informáticos o a redes conectadas con el Servicio, a través de búsqueda automática de contraseñas o por otros medios.

MODIFICACIONES AL SERVICIO

La oficina de sistemas de la E.S.E. Hospital San Rafael de Fusagasugá se reserva el derecho para modificar las condiciones aquí establecidas cuando lo considere necesario. También podrá modificar o incluso suspender el servicio o partes del mismo cuando sea necesario, por razones administrativas, de mantenimiento de los equipos o por causas de fuerza mayor.

CANCELACIÓN

La oficina de sistemas puede en cualquier momento cancelar o inhabilitar la cuenta de cualquier usuario e incluso eliminar su información por falta de uso, o bien si considera que el usuario ha contravenido las reglas aquí mencionadas.

POLÍTICAS PARA EVITAR CONTAMINACIÓN POR VIRUS A TRAVÉS DEL CORREO ELECTRÓNICO

- Revisar archivos con el antivirus antes de ser enviados como datos adjuntos.
- No abrir correos electrónicos de remitentes desconocidos o que le ofrezcan una promoción.
- Evitar abrir archivos adjuntos no solicitados.
- Vacunar los medios de almacenamiento extraíbles (USB, CD-DVD, entre otros), cada vez que se vaya a hacer uso de ellos.

- Mantener informados a los usuarios del hospital sobre nuevos virus que se encuentren en la red advirtiendo los daños que pueda causar.

PROCESO PARA PREVENIR PROBLEMAS DE VIRUS

Estas son algunas recomendaciones que debe tener en cuenta para proteger su equipo de algún ataque de un virus, recuerde que también es responsabilidad:

- No esconder extensiones de archivos tipos de programa conocidos: Todos los sistemas operativos Windows, por predeterminación, esconden la extensión de archivos conocidos en el Explorador de Windows. Esta característica puede ser usada por los diseñadores de virus y hackers para disfrazar programas maliciosos como si fueran otra extensión de archivo. Por eso los usuarios, son engañados, y dan clic sobre el archivo de "texto" y sin darse cuenta ejecutan el archivo malicioso.
- Configurar la seguridad de Internet Explorer como mínimo a "Media": Para activar esta función hay que abrir el navegador, ir a Herramientas, Opciones de Internet, Seguridad. Después elegir la zona correspondiente (en este caso Internet) y un clic en el botón Nivel Personalizado: allí hay que seleccionar Configuración Media o Alta, según el riesgo que sienta el usuario en ese momento.
- Hacer copias de seguridad: El disco duro es el medio de almacenamiento de los computadores personales. Pero desafortunadamente, suelen fallar. Cuando un disco duro colapsa, toda su información está en peligro. Algunas veces, la información puede recuperarse, pero es un procedimiento irritante y duradero que puede terminar sin resultados.
- Nunca trabaje un archivo directamente sobre un medio magnético, especialmente sobre un disquete o memoria USB ya que si este se daña por virus u otro problema la mayoría de las veces no podrá recuperar la información.
- Una copia de seguridad el archivo consiste en realizar una duplicación de la información a un segundo medio de almacenamiento en caso de que el primero falle. Este segundo medio de almacenamiento puede ser otro disco duro, CDS, DVD, memorias USB o un servidor de archivos.
- Actualizar el sistema operativo: Fundamental para aumentar al máximo la seguridad ante eventuales ataques de virus informáticos ya que muchos de los ataques que recorren el mundo buscan, especialmente, los sistemas operativos no actualizados. Para ello los proveedores de los sistemas operativos tanto de los equipos Servidores, como de los equipos clientes ofrecen periódicamente actualizaciones para descargar o también el usuario puede configurar Windows para que las descargue en forma automática.
- Cuidado con los archivos que llegan por correo: Al recibir un nuevo mensaje de correo electrónico, analizarlo con el antivirus antes de abrirlo, aunque conozca al remitente. Muchos virus se activan porque los usuarios abren los archivos adjuntos de los correos. Es preferible guardar los archivos en el disco local y luego rastrearlo con un antivirus actualizado (En vez de hacer doble clic sobre el archivo adjunto del correo entrante).
- Otras Recomendaciones:
    - Utilice el antivirus autorizado por el Hospital, el antivirus soportado estará disponible en la oficina de Sistema y será de uso exclusivo para los equipos de cómputo de la entidad, esto en razón a que es un antivirus licenciado.
    - No abrir archivos o macros adjuntas a un correo de procedencia desconocida, sospechosa o fuente no confiable, borre los archivos adjuntos inmediatamente, luego haga un doble borrado, vaciando su papelera de reciclaje.
    - Borrar el spam, cadenas y cualquier correo chatarra. Nunca realice reenvío de los mismos.
    - Nunca descargar archivos de sitios desconocidos o fuentes sospechosas.
    - Evitar compartir directamente los discos del computador con permisos de lectura / escritura, a menos que sea extremadamente necesario por la existencia de un requerimiento la entidad. Solo habilite una carpeta compartida y coloque allí los archivos que desee compartir.
    - Respaldar información crítica y configuración de sistemas en forma regular y almacenar la información en un lugar seguro.
    - También evitar descargar programas desde sitios de Internet que despierten sospechas o programas desconocidos.
    - Como la mayoría de usuarios transportan información personal y laboral en sus memorias USB o portátiles deben tener en cuenta que así el Hospital tenga un programa de antivirus en sus equipos deben tener en cuenta que otra puerta de entrada de virus son sus equipos personales. En estos casos

es necesario que sus equipos personales cuenten con un antivirus actualizado, recuerdo que estos también pueden estar en riesgo.

CONFIDENCIALIDAD

- Toda la información manejada en el hospital tal como oficios, actas, cartas, informes, proyectos, invitaciones públicas, etc. se consideran información confidencial y no deberá ser por ningún motivo difundidas
- Se debe custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidas.
- Los temas tratados en reuniones institucionales dentro del hospital solo son de interés del mismo y por lo tanto se considera información confidencial, la información debe ser utilizada exclusivamente para actividades relacionadas con las funciones propias de la organización.

5. BIBLIOGRAFÍA

- Departamento administrativo de la función pública 2018. Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planeas institucionales y estratégicos al plan de acción por parte de las entidades del estado". Bogotá, Colombia.
- Ministerio de tecnologías de la información y las comunicaciones 2016. Guía de gestión de riesgos. Bogotá, Colombia. Retrived from. Https://www.mintic.gov.co/gestionti/615/articles-5482_g7_gestion_riesgos.pdf

6. ANEXOS

- Formato de cronograma 2021 de plan de seguridad y privacidad de la información.

7. APROBACIÓN, CONTROL Y DISPOSICIÓN DEL DOCUMENTO

7.1. APROBACIÓN

	Nombre	Cargo	Fecha	Firma
Elaboró	SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS SAS	SISTEMAS	27-ENE-2021	
Revisó	DIEGO ANDRES CUCAITA MORALES	PROFESIONAL APOYO PLANEACIÓN	27-ENE-2021	
	JULIÁN NIETO BELTRÁN	PROFESIONAL APOYO PLANEACIÓN		
	JAIRO BOBADILLA MONTENEGRO	PROFESIONAL PROCESO PLANEACIÓN		
	ISIDRO ALBERTO GONZÁLEZ RODRÍGUEZ	SUBGERENTE ADMINISTRATIVO		
Aprobó	ANDRÉS MAURICIO GONZÁLEZ CAYCEDO	GERENTE	27-ENE-2021	

7.2. CONTROL DE CAMBIOS Y REVISIONES

Versión	Descripción del cambio o revisión	Nombre	Fecha	Firma
01	Creación del documento	JAVIER ANTONIO MELO RIVERA	03-SEP-2018	
02	Actualización de documento a la vigencia, se estructura el documento	SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS SAS	27-ENE-2021	

7.3. CONTROL DE COPIAS				
Copias	**Nombre de quien recibe**	**Cargo**	**Fecha**	**Firma**
Original	JAIRO BOBADILLA MONTENEGRO	PROFESIONAL PROCESO PLANEACIÓN	27-ENE-2021	

7.4. CONTROL Y DISPOSICIÓN DE REGISTROS DOCUMENTALES					
Identificación		**Área de almacenamiento**	**Conservación**		**Disposición final**
Código	**Nombre del documento**		**Archivo de gestión**	**Archivo central**	
SS-MA-03 V02	Plan de seguridad y privacidad de la información	Planeación institucional	2	8	Conservación total

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN