2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMAS

E.S.E. HOSPITAL SAN RAFAEL DE FUSAGASUGÁ

Hospital San Rafael de Fusagasugá

REGIÓN DE SALUD
SUR

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:
SUBPROCESO DE SISTEMAS

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN RAFAEL DE FUSAGASUGÁ
MACROPROCESO APOYO
PROCESO RECURSOS FISICOS
AÑO 2024

Aprobación: 25-ENE-2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Mediante la implementación del plan de seguridad y privacidad de la información se establecen los lineamientos como base fundamental para apoyar la preservación de la confidencialidad, integridad, disponibilidad de la información, dando cumplimiento permitiendo a la normatividad vigente en específico al decreto 612 de 2018 que reglamenta la integración de los planes institucionales y estratégicos al plan de acción, así como la gestión y mitigación de riesgos para la información.

La E.S.E. Hospital San Rafael de Fusagasugá trabaja en el fortalecimiento de la seguridad, 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.

La construcción del presente plan se realiza orientados por el modelo de seguridad y privacidad de la información – MSPI y modelo integrado de planeación y gestión MIPG

La E.S.E Hospital San Rafel de Fusagasugá impulsa Tecnologías de la Información y las Comunicaciones, con el ánimo de garantizar la interacción con la ciudadanía y funcionarios por medio del uso adecuado de los recursos que se tienen dispuestos para tal fin.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Potenciar la aplicación de buenas prácticas de gestión y uso de medios tecnológicos aplicables para la E.S.E. Hospital San Rafael de Fusagasugá adoptadas en la política de seguridad y privacidad de la información bajo el desarrollo de controles permanentes.

2.2. OBJETIVOS ESPECIFICOS

- Establecer un plan de comunicación que permita promover el uso de mejores prácticas de seguridad de la información en la institución.
- Incrementar el nivel de la seguridad de la información al interior de le entidad.
- Establecer actividades que permitan mitigar el impacto en cuanto a incidentes con la información y poder poner en práctica la seguridad digital.
- Incremento en la transparencia de la gestión pública.

- 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.
- Trabajar mancomunadamente con el plan estratégico institucional y la ejecución del plan estratégico de tecnologías de la información y de las comunicaciones.

3. ALCANCE

Las acciones y mecanismos contenidos en el Plan de Seguridad y Privacidad de la Información aplican para todos los procesos institucionales de la ESE HOSPITAL SAN RAFAEL DE FUSAGASUGÁ, Centros y Puesto de Salud, los cuales manejen, información institucional obtenida de la prestación de servicios de salud.

4. CONTENIDO

4.1. MARCO NORMATIVO

1. 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."

2. NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 tecnología de la información. Técnicas de de gestión de la seguridad de la información (SGSI)

3. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales."

4. 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. DIFINICIONES

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.

Amenaza: peligro potencial externo al activo. A diferencia de la vulnerabilidad, que es propia de la naturaleza del activo, las amenazas dependen de la exposición que pueda tener el activo.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Antivirus: es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas: son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware

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

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.

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

Ataque informático: Hace referencia a todo intento que se realiza para eludir los controles de seguridad en un sistema, cuyo propósito de evasión es comprometer el sistema con algún fin malicioso, es decir, afectar la disponibilidad, confidencialidad o integridad de la información (interrumpir la operación de un sistema, manipularlo para obtener algún tipo de ventaja que afecte a la organización, robar información etc.). Estos ataques son ideados por personas que utilizan sus conocimientos en informática para aprovechar las vulnerabilidades de un sistema.

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).

Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

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. DIAGNOSTIGO DE SEGURIDAD Y PRIVACIDAD

4.3.1. RESPONSABLES

Las responsabilidades para la gestión de plan de seguridad y privacidad de la información de la E.S.E. HOSPITAL SAN RAFAEL DE FUSAGASUGA, estarán a cargo de las siguientes áreas:

1. Subgerencia Administrativa
2. Calidad
3. Planeación
4. Oficina de Sistemas
5. Gestión Documental
6. Comunicaciones

4.3.2. POLÍTICA INSTITUCIONAÑ DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

4.3.2.1. **OBJETO:** Crear la Política Institucional de Gerencia de las Tecnologías de la Información y la Comunicación de la E.S.E. Hospital San Rafael de Fusagasugá en la cual:

"La ESE Hospital San Rafael de Fusagasugá se compromete a optimizar la implementación de herramientas digitales que promuevan las buenas prácticas de trabajo y rendimiento institucional, asegurando la conservación digital de la información, salvaguardándola de posibles amenazas y vulnerabilidades. Permitiendo de esta manera la autenticidad, confidencialidad, integridad y disponibilidad de la información, haciendo uso seguro de los datos personales captados con el fin de aportar a la toma de decisiones, mediante la participación, adopción y apropiación de las TICs en cumplimiento a los requisitos legales y reglamentarios."

4.3.2.2. **OBJETIVOS:** La política institucional de Gerencia de las Tecnologías de la Información y la Comunicación de la E.S.E. Hospital San Rafael de Fusagasugá está articulada con los siguientes objetivos estratégicos:

a) Gestión de la Tecnología: Diseñar, implementar, innovar y mejorar el proceso de gestión de la tecnología de acuerdo con el modelo integrado de planeación y gestión, que dé alcance a la identificación de las necesidades hasta su reposición y/o renovación.

b) Gestión estratégica de planeación y calidad: Fortalecer la gestión administrativa y de calidad en salud, fundamentado en la gestión por procesos, íntegros, trasparentes, innovadores y efectivos.

c) Gestión del riesgo: Implementar acciones continuas y sistemáticas para la prevención, mitigación y control de los riesgos que puedan afectar el desarrollo de la misión de la Empresa Social del Estado.

d) Gestión asistencial. Garantizar la prestación de servicios de salud humanizados, que cumplan los principios de accesibilidad, pertinencia, oportunidad, seguridad y continuidad.

e) Procesos Humanizados: Garantizar la prestación de servicios humanizados y centrados en el paciente.

f) Gestión de la Infraestructura: Realizar adecuación a la infraestructura a través del programa de mantenimiento físico, conforme a los requisitos de la normatividad vigente brindando seguridad y satisfacción a los grupos de valor.

Para dar cumplimiento a la presente política se establecen los siguientes objetivos:

4.3.2.3. OBJETIVO GENERAL:

Establecer procedimientos adecuados para la administración y buen manejo de los datos personales y la información institucional tanto física como digital aportando a la interoperabilidad con todos los procesos, haciendo uso y aprovechamiento de las tecnologías de la información y las comunicaciones aportando efectivamente a la autenticidad, integridad, confidencialidad y disponibilidad a través del tiempo.

4.3.2.4. OBJETIVOS ESPECÍFICOS:

Se determinan los siguientes objetivos específicos de La política institucional de Gerencia de las Tecnologías de la Información y la Comunicación de la E.S.E. Hospital San Rafael de Fusagasugá.

- Identificar los ataques cibernéticos que impidan la correcta prestación de los servicios con el fin de implementar acciones que permitan minimizarlos.
- Establecer los controles necesarios para el manejo y la gestión integral de los riesgos que pongan en vulnerabilidad la información, haciendo énfasis en fortalecer en los colaboradores la cultura de uso responsable de la información generando privacidad y seguridad de la información

- Establecer medidas institucionales que permitan una adecuada minería de datos, validación, consolidación, elaboración y radicación de informes institucionales normativos, municipales, departamentales, nacionales y otros que sirvan como insumo para evaluar resultados asistenciales administrativos y financieros que permitan a la alta gerencia tomar decisiones

- Conservar la documentación digital producida y recibida, en condiciones que garanticen la seguridad, disposición y consulta a través del tiempo.

- Establecer medidas de control que permitan fomentar custodia, tratamiento y confidencialidad en la protección de datos personales de los usuarios y colaboradores de la E.S.E Hospital San Rafael de Fusagasugá aportando al cumplimiento de la intimidad y la honra del buen nombre.

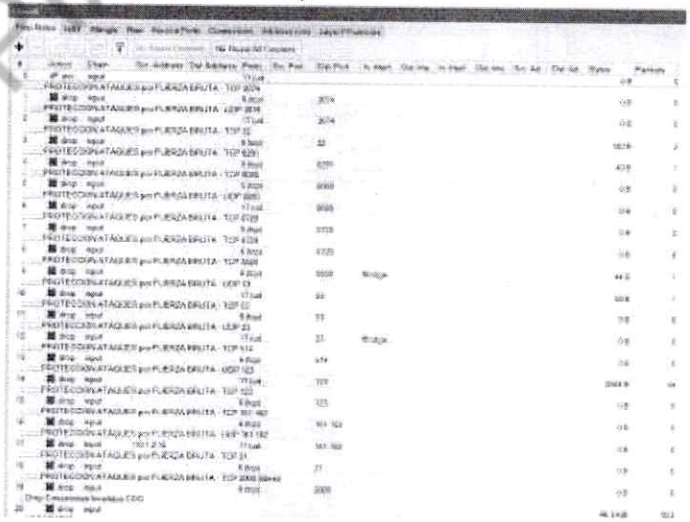
4.3.3. SEGURIDAD PERIMETRAL

Firewall

La E.S.E Hospital San Rafael de Fusagasugá utiliza un dispositivo MikroTika través del cual se pasa el tráfico de la red y que aceptan o deniegan el tráfico en base a unas políticas o reglas de acceso.

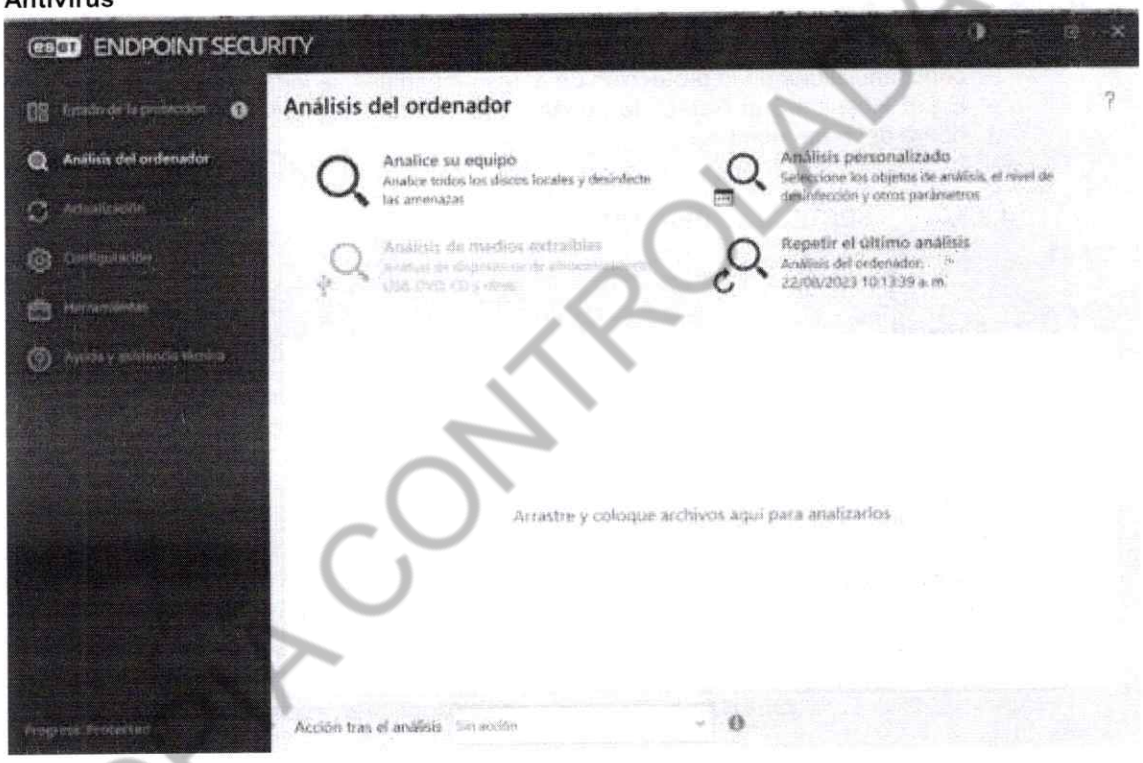
Funcionando este a dos niveles

– A nivel de red: permitiendo o denegando el tráfico en función de la IP de origen y de la IP de destino o a nivel de subredes (conjunto de IPs de origen y de IPs de destino).
– A nivel de aplicación: permitiendo o denegando el tráfico en función del protocolo utilizado en las comunicaciones (p. ej. DNS, NTP…).



Dentro de las políticas que se tienen establecidas por medio este Firewall se tiene restringido el uso de redes sociales como Facebook, Instagram, YouTube y mensajería instantánea como WhatsApp.

Antivirus



- Compatibilidad con todas las versiones de Windows – desde Vista hasta Windows10
- Un paquete especial para Mac, Linux y Android disponible
- Protección de alta calidad contra malware, virus, spyware y rescates
- Una función de escaneo de correo electrónico incorporada
- Un escaneo automático en tiempo real
- Protección contra el phishing
- Un módulo de protección AMSI para la rápida detección de código JS no deseado
- Un impacto medio del sistema
- Disponibilidad de paquetes premium para protección avanzada

4.4. PLAN DE SEGURIDAD Y PRIVACIDAD

Con el propósito de coordinar la seguridad física y lógica a la infraestructura y datos del Sistema de Información utilizado por el 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

4.4.1. LINEAMIENTOS

- **Uso, Instalación y Mantenimiento de Equipos De Cómputo.**

La estructura y uso de la red de datos, equipos de conectividad, equipos 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.

Estos lineamientos se han ido adoptando en cada proceso de la E.S.E Hospital San Rafael de Fusagasugá donde se hace necesaria la utilización de elementos de cómputo (computadores, impresoras y equipos de red) contribuyendo a una cultura, para el cuidado y adecuado funcionamiento de cada uno de estos equipos.

- **Condiciones generales de uso de los equipos de computo**

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 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 ESE.

Las actividades realizadas en los equipos de cómputo y con la red de datos de la E.S.E Hospital San Rafael de Fusagasugá 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 con 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, 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 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, impresoras y equipos de red), es obligación de los usuarios mantener limpias las áreas donde se encuentren equipos, Depositando la basura en los botes destinados para este fin.

• Evitar 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.

• Abstenerse 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, WhatsApp, Facebook, Yahoo Messenger u otros. Su omisión será reportada a la Oficina de Control Interno.

• Abstenerse 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 Departamento 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 de la E.S.E Hospital San Rafael de Fusagasugá tendrá 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**

• El 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,

• 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 de la ESE HSRC

• 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. (Anexo Nº 1)

• 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 líder de la oficina de Sistemas.

• Para las plataformas institucionales debe existir un único usuario con privilegios de administrador que será usada y administrada por el Líder de la oficina 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:

1. Programación del JOP en el motor de base de datos SQL Server
2. Programar la generación diaria de una copia de seguridad
3. Copia del archivo generado y se entregara una a subgerencia 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 del Hospital San Rafael 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.

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).

- **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

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.

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 los 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.

4.4.2. 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.

4.4.3. PLAN DE IMPLEMENTACIÓN

De la fase de implementación para el 2024 se tiene la siguientes programadas las siguientes actividades

- Documentar, mantener y divulgar procedimientos de tecnología, incluida la Política Institucional de Gerencia de las Tecnologías de la Información y la Comunicación, el uso de los servicios tecnológicos en toda la E.S.E Hospital San Rafael de Fusagasugá de acuerdo con los lineamientos establecidos en este plan.
- Respaldar la información que reposa en los diferentes sistemas de información, bases de datos, aplicativos y desarrollos propios.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica generando acciones para implementar correctivos
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la E.S.E Hospital San Rafael de Fusagasugá.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la E.S.E Hospital San Rafael de Fusagasugá.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los dalos e información gestionados.

4.4.4. ANALISIS DE RIESGO

Dentro del presente plan se realizará el análisis de riesgos a los que están expuestos los activos de la organización de la E.S.E Hospital San Rafael de Fusagasugá.

Activos de información

- Activos tangibles
- Activos intangibles

- Sistemas operativos, como servidores, ordenadores o dispositivos de red.
- Software utilizado en cualquier proceso

Activos físicos

- Infraestructuras de la organización
- Equipos de computo
- Hardware
- Equipos de control

Activos humanos:

- Empleados.
- Clientes.
- Contratistas
- Proveedores

El análisis de los riegos se realizará bajo los lineamientos establecidos en la norma ISO 31000 e ISO 27005:2008 realizando la Identificación de los activos de la información, caracterización de activos de la información: Se trata de identificar los activos definidos y los recursos que se dispone para la protección de estos.

Para el análisis de riesgos se tienen los siguientes conceptos:

- Una amenaza se trata del evento que puede corromper un activo a partir de una vulnerabilidad. Por tanto, sin vulnerabilidad, una amenaza no supone riesgo alguno.
- La amenaza más común es la humana, causando eventos independientemente de la intencionalidad.
- Existen amenazas naturales como falta de electricidad, desastres naturales, fallas de hardware/software.
- Se deben determinar todas las amenazas que pueden afectar a cada activo o grupo de activos.

Los riesgos identificados y su respectiva gestión se realizarán de acuerdo con el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5. BIBLIOGRAFÍA

GUIA DE GESTION DE RIESGOS. MINISTERIO. SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. MINISTERIO DE LAS TIC. http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

6. ANEXOS

Cronograma del plan

7. APROBACIÓN, CONTROL Y DISPOSICIÓN DEL DOCUMENTO

7.1. APROBACIÓN

	Nombre	Cargo	Fecha	Firma
Elaboró	DIANA MABEL PADILLA.	PROFESIONAL ESPECIALIZADO DE SISTEMAS	25-ENE-2024	
Revisó	YADIRA SILVA PAEZ	PROFESIONAL ESPECIALIZADO DE APOYO PLANEACIÓN	25-ENE-2024	
	ALEX FRANCISCO BOGOTA LOZANO	PROFESIONAL ESPECIALIZADO PLANEACIÓN		
	DIANA MARCELA FORERO DELGADO	SUBGERENTE ADMINISTRATIVO (E)		
Aprobó	ANDRES MAURICIO GONZALEZ CAYCEDO	GERENTE	25-ENE-2024	

7.2. CONTROL DE CAMBIOS Y REVISIONES

Versión	Descripción del cambio o revisión	Nombre	Fecha	Firma
1	Creación del documento	JAVIER ANTONIO MELO RIVERA	03-SEP-2018	
2	Actualización de documento a la vigencia, se estructura el documento	DIANA MABEL PADILLA.	27-ENE-2021	
3	Se actualiza el plan de tecnologías de la información y las	DIANA MABEL PADILLA.	31-ENE-2022	

	comunicaciones PETIC al contexto actual del hospital.			
4	Se actualiza plan de acuerdo a las necesidades de la vigencia 2023 y actualización de formato	DIANA MABEL PADILLA.	26-ENE-2023	
5	Se actualiza plan de acuerdo a las necesidades de la vigencia 2024	DIANA MABEL PADILLA.	25-ENE-2024	

7.3. CONTROL DE COPIAS

Copias	Nombre de quien recibe	Cargo	Fecha	Firma
Original	ALEX FRANCISCO BOGOTA LOZANO	PROFESIONAL ESPECIALIZADO PLANEACIÓN INSTITUCIONAL	25-ENE-2024	

7.4. CONTROL Y DISPOSICIÓN DE REGISTROS DOCUMENTALES

Identificación		Área de almacenamiento	Conservación		Disposición final
Código	Nombre del documento		Archivo de gestión	Archivo central	
RF-SS-PN-03 V05	Plan de seguridad y privacidad de la información	Planeación institucional	2	8	Conservación Total

RESOLUCION No. 025
(31 ENE 2024)

"Por medio de la cual se adopta el plan de privacidad y seguridad de la información, vigencia 2024 para la E.S.E. Hospital San Rafael de Fusagasugá y se determinan 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 Ley 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales"*, aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados y convenios internacionales.

Que la 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" regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.*

Que el decreto 1413 de 2017 *"Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales"*, establece los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos.

Que el 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"* estableciendo los instrumentos para implementar la "*Estrategia del Gobierno en Línea*", ahora Política de Gobierno Digital, exigiendo la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la Información que debe se integrado en el Plan de Acción, el cual debe ser publicado en el sitio web oficial de la Entidad.

Que el Decreto Único Reglamentario del Sector de Tecnologías de Información y las Comunicaciones define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

Que *el plan de privacidad y seguridad de la información* es el documento mediante el cual se define la estrategia bajo la cual se espera que las Tecnologías de la Información (TI) se integran con la misión, visión, y objetivos institucionales.

Que, conforme al marco de referencia del MinTIC, el plan de privacidad y seguridad de la información es parte integral de la estrategia de las instituciones y uno de los principales artefactos para expresarla, conformando su visión, estrategias y direccionando el resultado de un adecuado ejercicio de planeación, realizándose previamente a la definición de portafolios de proyectos y de un proceso de transformación que involucre tecnologías digitales. Que conforme a los principios de "Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones" y la "masificación del Gobierno en Línea", ahora Gobierno digital, consagrados respectivamente en los numerales 1 y 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deben priorizar el acceso y uso de las Tecnologías de la Información y las Comunicaciones (TIC) en la producción de bienes y servicios, así como adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información (TI) en el desarrollo de sus funciones, con el fin de lograr la prestación de servicios eficientes a los ciudadanos.

RESOLUCION No. 025
(31 ENE 2024)

"Por medio de la cual se adopta el plan de privacidad y seguridad de la información, vigencia 2024 para la E.S.E. Hospital San Rafael de Fusagasugá y se determinan otras disposiciones"

Que el Decreto Único Reglamentario del sector de la Función Pública, desde el decreto 1083 de 2015 y su modificación mediante el 1499 de 2017 y 612 de 2018 del departamento administrativo de la Función Pública, establece que los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público deben liderar la gestión estratégica de las TIC mediante la definición, implementación, ejecución, seguimiento y divulgación del plan de privacidad y seguridad de la información el cual debe estar alineado a la estrategia y al modelo integrado de la gestión de la entidad, teniendo un enfoque en la generación de valor público para habilitar las capacidades y servicios tecnológicos necesarios para impulsar las transformaciones, la eficiencia y la transparencia del Estado Que el decreto 612 de 2018 establece los instrumentos para implementar la "*Estrategia del Gobierno en Línea*", hoy Política de Gobierno Digital, exigiendo la elaboración por parte de cada entidad de un plan de privacidad y seguridad de la información que debe ser integrado en el Plan de Acción, el cual debe ser publicado en el sitio web oficial de la Entidad.

Que, en virtud de lo anterior, el comité institucional de gestión y desempeño de la E.S.E. Hospital San Rafael de Fusagasugá, en sesión ordinaria llevada a cabo el día 24 de enero de 2024 aprobó el plan de privacidad y seguridad de la información para la vigencia 2024.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO. OBJETO: Adoptar el Plan de Privacidad y Seguridad de la Información para la E.S.E. HOSPITAL SAN RAFAEL DE FUSAGASUGÁ, aprobado por el comité Institucional de Gestión y Desempeño, en sesión ordinaria del 25 de enero de 2024, para la vigencia 2024, plan que define la estrategia bajo la cual se espera que las Tecnologías de la Información (TI) se integran con la misión, visión y objetivos institucionales.

ARTÍCULO SEGUNDO. OBJETIVO:

2.1 OBJETIVO GENERAL: Potenciar la aplicación de buenas prácticas de gestión y uso de medios tecnológicos aplicables para la E.S.E. Hospital San Rafael de Fusagasugá adoptadas en la política de seguridad y privacidad de la información bajo el desarrollo de controles permanentes.

2.2 OBJETIVO ESPECÍFICOS:

- Establecer un plan de comunicación que permita promover el uso de mejores prácticas de seguridad de la información en la institución.
- Incrementar el nivel de la seguridad de la información al interior de le entidad.
- Establecer actividades que permitan mitigar el impacto en cuanto a incidentes con la información y poder poner en práctica la seguridad digital.
- Incremento en la transparencia de la gestión pública.
- 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.
- Trabajar mancomunadamente con el plan estratégico institucional y la ejecución del plan estratégico de tecnologías de la información y de las comunicaciones.

RESOLUCION No. 025
(31 ENE 2024)

"Por medio de la cual se adopta el plan de privacidad y seguridad de la información, vigencia 2024 para la E.S.E. Hospital San Rafael de Fusagasugá y se determinan otras disposiciones"

ARTÍCULO TERCERO. 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. **Amenaza:** peligro potencial externo al activo. A diferencia de la vulnerabilidad, que es propia de la naturaleza del activo, las amenazas dependen de la exposición que pueda tener el activo.

3.5. **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

3.6. **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

3.7. **Antivirus:** es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

3.8. **Aplicaciones engañosas:** son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

3.9. **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

3.10. **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.

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

3.12. **Ataque informático:** Hace referencia a todo intento que se realiza para eludir los controles de seguridad en un sistema, cuyo propósito de evasión es comprometer el sistema con algún fin malicioso, es decir, afectar la disponibilidad, confidencialidad o integridad de la información (interrumpir la operación de un sistema, manipularlo para obtener algún tipo de ventaja que

afecte a la organización, robar información etc.). Estos ataques son ideados por personas que utilizan sus conocimientos en informática para aprovechar las vulnerabilidades de un sistema.

3.13. **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

3.14. **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).

3.15. **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).

3.16. **Contraseña:** Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

3.17. **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.

3.18. **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)

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

3.20. **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).

3.21. **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).

3.22. **Datos Personales Mixtos**: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

3.23. **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).

3.24. 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).

3.25. 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).

3.26. 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)

3.27. Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

3.28. Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

3.29. 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).

3.30. 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.

3.31. 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)

3.32. 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).

3.33. 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).

3.34. Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

3.35. 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).

3.36. 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).

3.37. 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).

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

ARTÍCULO CUARTO. PRINCIPIOS:

4.1. Cada uno de los lineamientos, actividades y responsabilidades que se generen para aportar a la seguridad de la información serán definidas, compartidas, publicadas para conocimiento y puesta en práctica por cada uno de los funcionarios, contratistas, proveedores, o terceros de la E.S.E Se crearán estrategias para proteger.

4.2. Se generarán estrategias para que se proteja la información generada desde el sistema de información Dinámica Gerencial, así como la infraestructura tecnológica y activos del riesgo que se genera de los accesos indebidos.

4.3. Se crearán estrategias para proteger la información de las amenazas originadas por parte del personal.

4.4. Se crearán estrategias para proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, así como el control de acceso a la información, sistemas y recursos de red.

4.5. Gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información generando mejoras en la seguridad.

ARTÍCULO QUINTO. ESTRATEGIAS:

Dentro de la estrategia planteada por Gestión tecnológica se tiene:

5.1. Gestión de riesgos: Esta categoría incluye las actividades relacionadas con la identificación, evaluación y tratamiento de los riesgos de seguridad de la información. Las organizaciones deben contar con un proceso formal para identificar los riesgos a los que está expuesta su información, evaluar la probabilidad e impacto de estos riesgos, y tomar las medidas necesarias para mitigarlos.

5.2. Administración de la seguridad: Esta categoría incluye las actividades relacionadas con la implementación y mantenimiento de los controles de seguridad de la información. Los controles de seguridad son las medidas que se toman para proteger la información de los riesgos identificados. Las organizaciones deben contar con un conjunto de controles de seguridad adecuados para mitigar los riesgos a los que está expuesta su información.

5.3. Educación y concienciación: Esta categoría incluye las actividades relacionadas con la capacitación del personal en materia de seguridad de la información. El personal es un factor clave en la seguridad de la información, por lo que es importante que esté capacitado para identificar y reportar incidentes de seguridad.

- **Gestión de incidentes:** Esta categoría incluye las actividades relacionadas con la respuesta a los incidentes de seguridad de la información. Las organizaciones deben contar con un plan de respuesta a incidentes que les permita responder de manera efectiva a los incidentes de seguridad.

ARTÍCULO SEXTO. IMPLEMENTACIÓN: En la implementación, aplicación y seguimiento al plan 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:

6.1. SOCIALIZACIÓN: Se debe presentar al cierre de cada vigencia en el comité institucional de gestión y desempeño los avances obtenidos en cuanto al cumplimiento de los planes establecidos para su respectiva implementación, aplicación y seguimiento en cuanto al despliegue, apropiación y operación del plan estratégico de tecnologías de la información, plan de privacidad y seguridad de la información y plan de tratamiento de riesgos de seguridad y privacidad de la Información.

6.2. RESPONSABILIDAD: El plan 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 subgerente administrativo del hospital con apoyo del subproceso de sistemas.

ARTÍCULO SÉPTIMO. SEGUIMIENTO:

7.1. COMITÉ: Los avances obtenidos en cada vigencia, así como el cumplimiento el desarrollo de las estrategias establecidas para la implementación, aplicación y seguimiento en cuanto al despliegue, apropiación y operación de *plan de privacidad y seguridad de la información* de la E.S.E. Hospital San Rafael de Fusagasugá serán socializados en el comité de sistemas de información.

7.2. INDICADORES: Se realizará seguimiento a la implementación del plan a través de los siguientes indicadores.

Objetivo	Meta	Indicador	Tiempo de ejecución
Establecer un plan de comunicación que permita promover el uso de mejores prácticas de seguridad de la información en la institución.	90	Nombre: capacitación de colaboradores Formula: Número de colaboradores capacitados / Total de colaboradores solicitados *100	Anual
Incrementar el nivel de la seguridad de la información al interior de le entidad.	0%	Nombre: Porcentaje de ataques cibernéticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios. Fórmula: Número de ataques cibernéticos recibidos en el periodo que impidieron la prestación de algunos de los servicios/ Total de ataques cibernéticos recibidos en el periodo* 100	Anual
Establecer actividades que permitan mitigar el impacto en		Nombre: Porcentaje de riesgos materializados relacionados con la privacidad y seguridad de la información	Anual

cuanto a incidentes con la información y poder poner en práctica la seguridad digital.	0%	Formula: Número de riesgos materializados relacionados con la privacidad y seguridad de la información / Total de riesgos reportados relacionados con la privacidad y seguridad de la información en el periodo *100	

ARTÍCULO OCTAVO. ALCANCE: *el plan de privacidad y seguridad de la información* de la E.S.E. Hospital San Rafael de Fusagasugá, se hacen extensivos y aplican a todas las partes interesadas como cliente interno (servidores públicos, contratistas, personal en práctica formativa, personas jurídicas y proveedores) de los procesos, subprocesos y servicios de la sede central y sedes adscritas.

ARTÍCULO NOVENO. VIGENCIA Y DEROGACIONES: La presente resolución 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: Diana Mabel Padilla - Profesional Sistemas Soluciones Integrales y Desarrollos Informáticos S.A.S.
Revisó: Yadira Silva Páez - Profesional Especialización de Apoyo Planeación
Alex Francisco Bogotá - Profesional Especializado de Planeación.
Daniel Arturo Bobadilla A. - Abogado Oficina Jurídica (Revisa aspectos jurídicos)
Aprobó: Diana Marcela Forero Delgado - Subgerente Administrativo (E)
David Alberto Rojas Flórez - Subgerente Científico.
Diana Marcela Forero Delgado – Subgerente Comunitaria