PLAN DE SEGURIDAD
DE LA INFORMACION

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, por medio de la Estrategia de Gobierno en línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

2. INTRODUCCIÓN

La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene EL HOSPITAL SAN RAFAEL E.S.E defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Gerencia.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad.

Actualmente la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) cuenta con una plataforma tecnológica que almacena, procesa y transmite la información institucional, incluye equipos de cómputo de usuario y un servidor que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Siendo la información institucional un activo valioso para la empresa, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

3. ALCANCE

Las políticas de seguridad informática están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios de planta como por los contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), y por quienes hagan uso de los servicios tecnológicos de la empresa.

4. OBJETIVO

Definir e implementar las políticas de seguridad informática que dan las pautas y rigen para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), para su interiorización, aplicación y verificación permanente

5. TERMINOS Y DEFINICIONES

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Activo: Según [ISO IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del EL HOSPITAL SAN RAFAEL E.S.E . Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el EL HOSPITAL SAN RAFAEL E.S.E . Ejemplo: archivo de Word “listado de personal.docx”.

- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: Simens, Awa, Orfeo.

- **Personal:** Es todo el personal del EL HOSPITAL SAN RAFAEL E.S.E , el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del EL HOSPITAL SAN RAFAEL E.S.E . Ejemplo: Pedro Pérez.
- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.

- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones

Ejemplo: equipo de cómputo, teléfonos, impresoras.

- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina de sistemas.

- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Almacenamiento en la Nube: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

Amenaza: Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Cifrar: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - **Sistema de Gestión de la Seguridad de la Información**.

Cómputo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Declaración de aplicabilidad (SOA - Statement of Applicability): Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evento: Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

FTP: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

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.

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.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red[1] o faciliten información con clasificación confidencial o superior.

En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información. **Keyloggers:** Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al

Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Punto Único de Contacto (PUC): Entiéndase como mesa de ayuda de acuerdo a las mejores prácticas basadas en ITIL.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha

comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Tratamiento de riesgos: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del EL HOSPITAL SAN RAFAEL E.S.E , debidamente autorizados para usar equipos, sistemas o

aplicativos informáticos disponibles en la red del EL HOSPITAL SAN RAFAEL E.S.E y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Gerencia de EL HOSPITAL SAN RAFAEL E.S.E , entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para EL HOSPITAL SAN RAFAEL E.S.E , la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de EL HOSPITAL SAN RAFAEL E.S.E
- Garantizar la continuidad del negocio frente a incidentes.
- EL HOSPITAL SAN RAFAEL E.S.E ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

7. POLÍTICAS GENERALES DE SEGURIDAD FÍSICA

a. Se destinará un área en la empresa que servirá para la ubicación del servidor, debidamente protegido con la infraestructura apropiada, de manera que se restrinja el acceso directo a usuarios no autorizados. b. El área del servidor deberá contar con sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados, así como sistema eléctrico de respaldo (UPS).

c. Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

d. Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

e. Contar por lo menos con dos extintores de incendio adecuado y cercano al área del servidor.

f. Los equipos que hacen parte de la infraestructura tecnológica de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

8. POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS

8.1. Gestión de la Información:

a. Todo empleado de planta o contratista que inicie labores en la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en el Manual de Políticas de Seguridad Informática.

b. Los empleados que se desvinculen y los contratistas que culminen su vínculo contractual con la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), deberán hacer entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para expedición de paz y salvo y/o liquidación de contrato.

c. Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), por lo tanto,

no se hará divulgación ni extracción de la misma sin previa autorización de las directivas de la empresa.

d. No se realizará por parte de los empleados o contratistas copia no autorizada de información electrónica confidencial y software de propiedad de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). El retiro de información electrónica perteneciente a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) y clasificada como confidencial, se hará única y exclusivamente con la autorización del Gerente o su delegado.

e. Ningún empleado o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

f. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

8.2. Hardware y Software:

a. La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del área de Sistemas de Información.

b. El espacio en disco duro de los equipos de cómputo pertenecientes a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video).

c. Ningún empleado o contratista podrá acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la persona responsable.

d. Ningún empleado o contratista podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

e. Ningún empleado o contratista podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, salvo el personal autorizado del área de Sistemas de Información en aplicación de las políticas o medidas de seguridad.

f. No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), para actividades que no estén relacionadas con las labores propias de La empresa.

g. Los empleados y contratistas serán responsables de contar con conocimientos actualizados en informática básica y el uso de herramientas ofimáticas.

8.3. Correo Electrónico:

a. El correo electrónico institucional es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en la empresa.

b. La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca).

c. Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

d. Es responsabilidad del empleado o contratista depurar su cuenta de correo periódicamente, en todo caso se debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

8.4. Internet:

a. No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la empresa.

b. El Servicio de internet de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la empresa. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

c. No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) o de las personas.

d. ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la empresa.

8.5. Cuentas de Acceso:

a. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada empleado y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única

y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca).

b. Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.

c. La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínimo cada 4 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

d. Solamente puede solicitar cambio o restablecimiento de contraseña desde el servidor el empleado o contratista al cual pertenece dicho usuario, o el Líder inmediato mediante solicitud motivada al correo electrónico del área de Sistemas de Información.

e. Todo empleado o contratista que se retire de la empresa de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o al Líder del proceso de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

8.6. Seguridad Física:

a. Es responsabilidad de los empleados y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la empresa única y exclusivamente con autorización de gerencia o subgerencia y diligenciando el formato de movimientos de activos fijos firmado por subgerencia y estrictamente para ejercer labores que estén relacionadas con la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normatividad para tal fin.

b. Los empleados y contratistas deberán reportar de forma inmediata a los directivos la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

c. Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas.

d. Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

8.7. Derechos de Autor:

a. Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

8.8. Uso de Unidades de Almacenamiento Extraíbles:

a. Los empleados y contratistas que tengan información de propiedad de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

b. Toda información que provenga de un archivo externo de la empresa o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

8.9. Clasificación de la información:

a. Los documentos electrónicos resultantes de los procesos misionales y de apoyo de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), se tratarán conforme a los lineamientos y parámetros establecidos en el Sistema de Gestión Documental de la empresa. Los activos de información asociados a cada sistema de información serán identificados y clasificados por su tipo y uso siguiendo lo establecido en el Listado Maestro de Documentos vigente.

8.10. Personal de Sistemas:

a. El control de los equipos tecnológicos deberá estar bajo la responsabilidad del área de Sistemas de Información, así como la asignación de usuarios y la ubicación física.

b. En el área de Sistemas de Información se deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

c. El área de Sistemas de Información será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

d. Las licencias de uso de software estarán bajo custodia del área de Sistemas de Información. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

e. El área de Sistemas de Información es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

f. Todas las publicaciones que se realicen en el sitio WEB de la entidad, deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

g. El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y contraseña. El área de Sistemas de Información será la encargada de crear y asignar las cuentas de acceso y sus permisos a dominio de red,

sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

h. Se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, garantizando la estandarización por cada usuario; es decir, que cada usuario debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones de la empresa. La estandarización de los nombres de usuario estará compuesta de la siguiente forma: (Primer letra del primer nombre + primer apellido, en caso de existir duplicidad, Primeras dos letras del primer nombre + primer apellido).

i. Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al retiro de los funcionarios o contratistas, debe aplicarse la inactivación del usuario.

j. Se realizará backup a la información institucional y bases de datos, conforme a lo establecido en la política de backup y cronograma, así como en los casos extraordinarios: desvinculación de funcionario o contratista, envío de equipo para garantía, mantenimiento correctivo de equipo.

k. Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la Entidad, deberán ser salvaguardadas por el área de Sistemas de Información en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

l. La red interna de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red.

m. Todos los equipos de la entidad deben tener instalado un antivirus, en funcionamiento, actualizado y debidamente licenciado.

n. Se realizará mantenimiento lógico preventivo a los equipos de cómputo mínimo cada 6 meses y mantenimiento físico preventivo mínimo una vez por año, que incluya el cableado estructurado. El área de Sistemas de Información deberá elaborar el plan y cronograma de mantenimientos, el cual será notificado a los usuarios, adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos e información.

8.11. Directivos:

a. La empresa debe garantizar capacitación a los empleados en el manejo del software de gestión, plataformas y aplicativos implementados en la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca).

b. Deberá notificarse al área de Sistemas de Información las novedades de vinculación y desvinculación de personal de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), con el fin de crear o cancelar, según sea el caso, los accesos a los sistemas de información, correo electrónico y red de datos.

9. POLÍTICAS ORIENTADAS A LOS USUARIOS EXTERNOS

a. El acceso de terceras personas a la empresa debe ser controlado y su ingreso a las diferentes dependencias debe ser autorizado por los empleados a cargo.

10. POLÍTICA DE ADMINISTRACIÓN DE BACKUP

10.1. Objetivo: Establecer las directrices para la ejecución y control de las copias de seguridad de la información digital perteneciente a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca).

10.2. Alcance: Estas directrices son aplicables a la información institucional, bases de datos y archivos de restauración de los equipos pertenecientes a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca).

10.3. Clasificación de la Información Institucional: Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), su producción, almacenamiento y gestión está a cargo de cada uno de los empleados y contratistas. Información que se encuentra alojada en los equipos de cómputo.

Bases de Datos: Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). La ESE cuenta con base de datos del software simens, awa y orfeo.

Archivos de Restauración del Sistema: Los archivos de restauración son la copia de las unidades necesarias para que se ejecute el Sistema Operativo, son la herramienta para recuperar el Sistema Operativo de un error grave o restaurar el equipo si la unidad de disco duro o el equipo dejan de funcionar.

10.4. Periodicidad del Backup

TIPO DE INFORMACIÓN	FRECUENCIA DE COPIA
Información Institucional	Una vez por semana
Bases de Datos	Tres veces por semana
Archivos de Restauración del Sistema	Semestral

- Informacion Institucional se va a realizar una vez por semana a traves de carpeta compratida en el servidorhsr y disco duro extraible.

- Las bases de datos se hara copia de seguridad tres veces por semana atraves del disco duro del servidorhsr y disco duro extraible.

10.5. Medios de Almacenamiento: Las copias de seguridad son almacenadas en un Disco Duro extraíble dispuesto exclusivamente para este fin. Este debe ser resguardado por el Líder de Gestión Sistemas de Información.

10.6. Control de los Backups: Cada copia de seguridad realizada debe ser registrada en los formatos F-113-05 y F-113-08. Se genera un expediente que permita el control de las copias realizadas y facilite la restauración de la información en caso de desastre.

10.7. Tipos de Backup: Las copias de seguridad se realizarán bajo el método de backup completo y backup incremental.

Backup completo: se hace un respaldo completo de todos archivos del equipo. La copia de seguridad abarca el 100% de los datos.

Backup incremental: se hace una copia de todos los archivos que han sido modificados desde que fue ejecutado el último backup completo.

11. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB El sitio web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) tiene como función principal proveer información y servicios, así como divulgar y promover normas y directrices internas y del Gobierno Nacional relacionadas con el sector salud. Conforme a los lineamientos del direccionamiento estratégico la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) publica los temas y actividades que tienen que ver con su misión, visión, objetivos y funciones por medio de su página www.hospitalsanrafaelcerrito.gov.co, informando sobre: trámites, servicios, indicadores de gestión, planes y programas, publicaciones, normas, convocatorias, información presupuestal, enlaces institucionales y, en general, información relacionada con los servicios y programas de salud que presta. La ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) solicita al visitante y al usuario de esta página que lea detalladamente estas condiciones y la política de privacidad, antes de iniciar su exploración o utilización. Si no está de acuerdo con estas condiciones de uso, le sugerimos que se abstenga de acceder o navegar por la página web de nuestra entidad. Así mismo, es importante aclarar que la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no persigue ningún lucro, ganancia o interés comercial con los contenidos o vínculos que se publican en su página web www.hospitalsanrafaelcerrito.gov.co

11.1. Aceptación de Términos: Se presume que cuando un usuario accede al sitio web de la www.hospitalsanrafaelcerrito.gov.co lo hace bajo su total responsabilidad y que, por tanto, acepta plenamente y sin reservas el contenido de los siguientes términos y condiciones de uso del sitio web de la entidad. Esta declaración de uso adecuado de la información está sujeta a los términos y condiciones de la página web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), con lo cual constituye un acuerdo legal entre el usuario y la página de la ESE. Si el usuario utiliza los servicios de la página web de la ESE, significa que ha leído, entendido y aceptado los términos expuestos. Si no está de acuerdo con ellos,

tiene la opción de no proporcionar ninguna información personal, o no utilizar el servicio de la página web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), www.hospitalsanrafaelcerrito.gov.co.

11.2. Condiciones generales respecto al contenido del sitio web

a. ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) se reserva, en todos los sentidos, el derecho de actualizar y modificar en cualquier momento y de cualquier forma, de manera unilateral y sin previo aviso, las presentes condiciones de uso y los contenidos de la página web www.hospitalsanrafaelcerrito.gov.co.

b. El sitio web tiene por finalidad brindar al usuario todo tipo de información relacionada con la gestión de prestación de servicios de salud en la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). La información contenida en esta página web, está redactada de forma breve, sencilla y clara, en formato de contenidos para web. La ESE procurará que la información satisfaga las necesidades de los usuarios.

c. El sitio web puede tener enlaces a otros sitios de interés o a documentos localizados en otras páginas web de propiedad de otras entidades, personas u organizaciones diferentes a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). En estos casos el usuario deberá someterse a las condiciones de uso y a la política de privacidad de las respectivas páginas web.

d. ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no se hace responsable respecto a la información que se halle fuera de este sitio web y no sea gestionada directamente por el administrador del sitio web www.hospitalsanrafaelcerrito.gov.co.

e. Los vínculos (links) que aparecen en el sitio web tienen como propósito informar al usuario sobre la existencia de otras fuentes susceptibles de ampliar los contenidos que ofrece la página web o que guardan relación con ellos.

f. ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no garantiza ni se responsabiliza del funcionamiento o accesibilidad de las páginas web vinculadas. Tampoco sugiere, invita o recomienda la visita a las mismas. Por eso, no será responsable del resultado obtenido.

g. El establecimiento de un vínculo (link) con el sitio web de otra empresa, entidad o programa no implica necesariamente la existencia de relaciones entre ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) y el propietario del sitio o página web vinculada, ni la aceptación o aprobación por parte de la ESE de sus contenidos o servicios.

h. Al ubicar en un sitio web el vínculo (link) de la página de ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), se deberá asegurar que direccione a la página de inicio.

i. Las personas que usen el vínculo (link) de la página de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), deberán abstenerse de realizar manifestaciones o indicaciones falsas, inexactas o incorrectas sobre la ESE o incluir contenidos ilícitos, o contrarios a las buenas costumbres y al orden público.

j. Las investigaciones publicadas en la página web de ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no implican, de parte de la empresa, juicio alguno o comprometen la posición de la entidad y/o de quienes intervienen en ella. Los contenidos son responsabilidad de quienes realizaron la investigación.

k. La prestación del servicio del sitio web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) es de carácter libre y gratuito para los usuarios y se rige por los términos y condiciones que aquí se incluyen, los cuales se entienden como conocidos y aceptados por los (las) usuarios (as) del sitio.

11.3. Derechos de autor de los contenidos de la página web – Copyright. Este sitio de internet y su contenido son de propiedad intelectual de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). Es posible descargar material de www.hospitalsanrafaelcerrito.gov.co para uso personal y no comercial, siempre y cuando se haga expresa mención de la propiedad en cabeza de la ESE. Respecto a los contenidos que aparecen en el sitio web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), el usuario se obliga a:

a. Usar los contenidos de forma diligente, correcta y lícita.

b. No suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifican los derechos de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca).

c. No emplear los contenidos y en particular la información de cualquier otra clase obtenida a través de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) o de los servicios, para emitir publicidad.

d. ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no será responsable por el uso indebido que hagan los usuarios del contenido de su sitio web.

e. El visitante o usuario del sitio web se hará responsable por cualquier uso indebido, ilícito o anormal que haga de los contenidos, información o servicios del sitio de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca). El visitante o usuario del sitio, directa o por interpuesta persona, no atentará de ninguna manera contra el sitio web de la ESE, contra su plataforma tecnológica, contra sus sistemas de información ni tampoco interferirá en su normal funcionamiento.

f. El visitante o el usuario del sitio no alterará, bloqueará o realizará cualquier otro acto que impida mostrar o acceder a cualquier contenido, información o servicios del sitio web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), o que estén incorporados en las páginas web vinculadas.

g. El visitante o el usuario del sitio web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no enviará o transmitirá en este sitio o hacia el mismo a otros usuarios o a cualquier persona cualquier información de alcance obsceno, difamatorio, injuriante, calumniante o discriminatorio.

h. El visitante o el usuario del sitio web de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) no incurrirá en y desde el mismo en conductas ilícitas, como daños o ataques informáticos, interceptación de comunicaciones, infracciones a los derechos de

autor, uso no autorizado de terminales, usurpación de identidad, revelación de secretos o falsedad en los documentos.

11.4. Ley Aplicable y Jurisdicción El usuario no podrá manifestar ante la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) o ante una autoridad judicial o administrativa, la aplicación de condición, norma o convenio que no esté expresamente incorporado en las presentes condiciones de uso. Estas condiciones serán gobernadas por las leyes de la República de Colombia, en los aspectos que no estén expresamente regulados en ellas. Si cualquier disposición de estas condiciones pierde validez o fuerza obligatoria, por cualquier razón, todas las demás disposiciones, conservan su fuerza obligatoria, carácter vinculante y generarán todos sus efectos. Para cualquier efecto legal o judicial, el lugar de las presentes condiciones es el Municipio de El Cerrito, Departamento del Valle del Cauca, República de Colombia, y cualquier controversia que surja de su interpretación o aplicación se someterá a los jueces de la República de Colombia.

11.5. Duración y terminación La prestación del servicio del sitio WEB de la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) tiene una duración indefinida. Sin embargo, la ESE podrá dar por terminada o suspender la prestación de este servicio en cualquier momento. En caso de que se llegue a presentar esta situación, la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) informará previamente sobre el hecho, para evitar mayores traumatismos.

11.6. Contáctenos Si el usuario desea hacer sugerencias a la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca) para mejorar los contenidos, la información y los servicios que se ofrecen en el sitio web www.hospitalsanrafaelcerrito.gov.co.com debe dirigirse al administrador de la página, en el siguiente correo electrónico: sistemas@hospitalsanrafaelcerrito.gov.co.

12. CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA la ESE HOSPITAL SAN RAFAEL de El Cerrito (Valle del Cauca), los directivos, los Líderes de Gestión, el Proceso de Sistemas de Información, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

13. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN:

Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano, el compromiso de la alta dirección en destinar los recursos

suficientes para desarrollar los programas y esta politica debe ser sensibilizada a todo el personal humano del Hospital San Rafael E.S.E.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	NATURALEZA DEL CAMBIOS	SELLO DE VIGENCIA
1		Creación del documento	

REVISADO POR:	APROBADO POR:
CARGO:	CARGO:

- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Definir los roles y responsabilidades de quienes diseñaran los programa, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios usuarios como las siguientes:
    - Política De Escritorio Limpio
    - Política De Uso Aceptable
    - Ética Empresarial.