TABLA DE CONTENIDO

1. POLÍTICA

La ESE Hospital San José del Guaviare, reconoce la información como un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la institución y para la atención de los pacientes. Este activo debe ser adecuadamente protegido, mediante las medidas de seguridad necesarias, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su captura, conocimiento, procesado y tratamiento, por lo tanto, se preocupa por establecer lineamientos que permitan mitigar los posibles riesgos para la Información.

La institución entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de un Sistema de gestión de la 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.

2. MARCO NORMATIVO

- **Resolución 1995 de 1999:** “Por la cual se establecen normas para el manejo de la Historia Clínica”
- **ISO 27001 del 2013**: Sistema de gestión de seguridad de la información
- **Ley 2015 del 31 de enero de 2020:** Por medio del cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones

3. MARCO CONCEPTUAL

- **La Historia Clínica:** Es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

- **Integralidad**: La historia clínica debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordándolo como un todo en sus aspectos biológico, psicológico y social, e interrelacionado con sus dimensiones personal, familiar y comunitaria.
- **Disponibilidad:** Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley.
- **Oportunidad**: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.
- **Activos de información**: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.
- **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo, Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Propietario/responsable de activo de información**: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- **Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.
- **Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por un sistema informático o producto de software, de esta manera el sistema puede diferenciar a cada usuario por medio de sus credenciales (usuario y contraseña) y así mismo relacionar registros de movimientos y permisos de accesos para operar en el mismo.
- **Amenaza:** Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.

- **Control de Acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.
- **Cracking**: Conducta delictiva en la cual un individuo se infiltra ilegalmente en sistemas informáticos (denominado cracker o pirata informático) y alteran, modifican o eliminan, los datos de un programa o documento informático con la finalidad de obtener un beneficio de dicha alteración.
- **Hardware:** Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
- **Software:** Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.
- **Vulnerabilidad:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
- **Virus informático:** software que tiene como objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario para lograr fines maliciosos sobre el dispositivo.

4. JUSTIFICACION

La utilización creciente de las Tecnologías de la información y las Comunicaciones ha generado beneficios para las instituciones, mejorando el cumplimiento de la misión y la prestación de servicios a la ciudadanía. Sin embargo, por ser la información el activo más importante de una organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, esto con fin de garantizar la seguridad de la información, en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la misma.

La política de seguridad de la información surge como una herramienta organizacional necesaria para concientizar a cada uno de los funcionarios de la institución sobre la importancia de la generación, trasferencia, conservación y uso de la información, por lo cual se debe garantizar el mínimo de riesgo y un alto grado de seguridad que favorezca el desarrollo de la organización, que permita su óptimo funcionamiento y el buen uso de la misma, a través de personas idóneas, capacitadas, procesos implementados y evaluados, backups de seguridad, equipos tecnológicos y de comunicación, permitiendo la recuperación de la información en el menor tiempo posible en caso de incidentes o eventos catastróficos.

Las principales amenazas que pueden presentar el Sistema de gestión de la seguridad de la información son: Uso indiscriminado de la Internet, mala práctica de los usuarios, descuido en la manipulación de los equipos y el desconocimiento de conceptos básicos de manejo de dispositivos informáticos. Es por eso, que esta política busca determinar los lineamientos para la protección de las redes, los datos y los equipos de la Institución.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Los lineamientos que se establezcan en esta política se constituyen como eje fundamental para la implementación de un Sistema de gestión de la seguridad de la información de la E.S.E Hospital San José del Guaviare y se convierten en la base para la implantación de controles, procedimientos y estándares, que contribuyen a la prevención, protección y manejo de los riesgos de seguridad en diversas circunstancias.

5. OBJETIVO GENERAL

Proteger los activos de información de la ESE Hospital San José del Guaviare, a través de la estandarización de lineamientos para la implementación de un sistema de gestión de la información, en el cual se establezcan controles para disminuir los riesgos potenciales de perdida de información sensible e importante para la institución, permitiendo satisfacer las necesidades de información y su interrelación con los diferentes clientes.

6. ALCANCE

Esta política aplica para TODOS los procesos institucionales, desde la generación de la información hasta el tratamiento, análisis y almacenamiento de la misma.

7. METODOLOGIA

A través de los lineamientos establecidos en la presente política la ESE Hospital San José del Guaviare, busca establecer controles con el fin de disminuir el riesgo el riesgo potencial de pérdida información o violación a la privacidad de la

misma, es por esto que se establecen los siguientes lineamientos y estrategias, las cuales deben ser gestionadas por todos los colaboradores de la institución.

Principios de seguridad de la información:

- Esta institución afronta la toma de riesgos y tolera aquellos que, en base a la información disponible, son comprensibles, controlados y tratados cuando es necesario. Los detalles de la metodología adoptada para la evaluación del riesgo y su tratamiento se encuentran descritos en la política del SGSI.
- Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
- Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento.
- Se tendrán en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
- Se harán disponibles informes regulares con información de la situación de la seguridad.
- Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
- Los criterios para la clasificación y la aceptación del riesgo se encuentran referenciados en la política del SGSI.
- Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.

7.1 LINEAMIENTOS

Para efectos de comprensión y estructuración de este documento, el área de sistemas de Información de la ESE Hospital San José del Guaviare, establece los siguientes lineamientos:

- Seguridad de los equipos.
- Seguridad de los Usuarios.
- Seguridad del Software.
- Seguridad de las Redes e Internet.

- Seguridad de los Datos e Información.
- Administración de seguridad Informática.
- Acuerdos sobre confidencialidad
- Controles de acceso físico

a. ESTRATEGIAS

SEGURIDAD DE LOS EQUIPOS

Los equipos son la parte fundamental para el almacenamiento y gestión de la información. La función de la Oficina de Sistemas de Información es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas en caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura informática. Es por esto que se deben establecer estrategias para:

- Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de la ESE Hospital San José del Guaviare, sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas de Información, de lo contrario no le será permitido conectar su equipo o dispositivo. Para los equipos que no sean propios de la ESE Hospital San José del Guaviare, se debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica.
- Los responsables de las áreas de activos fijos, mantenimiento, deberán en conjunto con la Oficina de Sistemas dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

- Cualquier equipo, periférico o accesorio de propiedad de la institución que necesite ser retirado de la entidad tendrá que autorizarlo la oficina de activos fijos, la cual solicitará el visto bueno de la oficina de sistema de información y subgerencia gestión administrativa y financiera.

- Todo equipo de la Institución, debe estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben

proporcionarse en conjunto con el área de mantenimiento. En general, todos los equipos, periféricos y accesorios computacionales deben estar lejos de los siguientes factores principales: La luz directa del Sol y de humedades, filtraciones y demás medios que puedan hacer que el equipo tenga contacto con el agua.

- Todo equipo o periférico perteneciente a la institución, deberá contar con un dispositivo de protección eléctrica, ya sea estabilizador de corriente o UPS, que resguarde al equipo ante un cambio brusco en la corriente eléctrica de la entidad o del sector donde se ubica. Por lo anterior, todo equipo propiedad de la institución, y que no cuente con alguno de estos dispositivos de protección, no puede ponerse en funcionamiento. Si el funcionario conectara el equipo, será el directo responsable de los daños que puedan ocurrirle a este. En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento de un funcionario de la oficina de Sistemas de Información.
- Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original. Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa de la oficina de Sistemas de Información, que evaluará la viabilidad de dicho cambio.
- La protección física y la limpieza interna y externa de los equipos corresponde al funcionario de la oficina de sistemas de información al que se le asigne la tarea, y la custodia y cuidado en el sitio de trabajo le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de Sistemas de Información.
- Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás. En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente a la oficina de Sistemas de Información quien hará el mantenimiento necesario he informara a quien corresponda para que se tomen las medidas correctivas necesarias.
- No se permite el uso de dispositivos de almacenamiento extraíble tales como memorias USB, CD o DVD, nuevas tecnologías en los equipos, salvo en aquellos casos en donde por fuerza mayor se requiera y previamente evaluado y aprobado por la oficina de Sistemas de Información. Para garantizar lo anterior, la oficina de Sistemas de Información bloquea los puertos USB (solamente para el uso de memorias), y las unidades de CD/DVD, si algún usuario necesita que ese bloqueo sea levantado, deberá solicitarlo a la oficina de Sistemas de Información.

- Toda instalación de equipo, mantenimiento o proceso de soporte técnico a nivel de hardware, sin importar su nivel de complejidad, debe ser única y exclusivamente realizado por personal de la oficina de Sistemas de Información. Bajo ningún concepto se autoriza que personal ajeno a la oficina de Sistemas de Información manipule los equipos.
- Para solicitar servicio de mantenimiento a un equipo, periférico o accesorio, se debe diligenciar un formato mantenimiento establecido (Ver formato de solicitud y reporte de soporte técnico versión 1.0 código A-IS-FO-01)
- Los equipos de cómputo no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) bajo ninguna causa. Está totalmente prohibido a los usuarios destapar o desarmar los equipos o impresoras bajo cualquier motivo, sin exclusión. El único personal autorizado para esta labor, es el de la oficina de Sistemas de Información. De detectarse que se está presentando esta conducta se informara y se tomaran las medidas correctivas necesarias.
- No se puede dar mantenimiento o soporte técnico a nivel de hardware a un equipo de cómputo que no es propiedad de ESE Hospital San José del Guaviare.
- Los funcionarios de la oficina de Sistemas de Información son los únicos autorizados para manejar, mantener y velar por la integridad y seguridad de los servidores centrales de la institución, a su vez de salvaguardar las credenciales de acceso a estos.
- El servidor central de la red de la ESE Hospital San José del Guaviare debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la oficina de Sistemas de Información, y con las condiciones adecuadas de espacio, temperatura, iluminación, suministro eléctrico ininterrumpido, entre otras.
- Los equipos propiedad del Hospital deben usarse solamente para las actividades propias de la ESE Hospital San José del Guaviare, por lo tanto, los usuarios no deben usarlos para asuntos personales. (Delito contra los bienes de la administración pública).
- La adquisición de nueva infraestructura de procesamiento de la información (hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser verificada por la Oficina de Sistemas de Información y el jefe de la oficina afectada.
- Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo.
- Todo equipo de cómputo que este asignado a áreas asistenciales y requiera ser retirado del servicio para mantenimiento, reparación, reubicación o reemplazo, debe previamente pasar por un proceso de desinfección en sitio, con el fin de prevenir posible contaminación.

SEGURIDAD DE LOS USUARIOS

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas de Información establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática.

Todos los funcionarios y contratistas de la ESE Hospital San José del Guaviare, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente, durante el proceso de vinculación deberán recibir inducción sobre lo establecido en esta política y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por el Hospital. La información almacenada en los equipos de cómputo del Hospital es propiedad de la institución y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información.

- Toda información en formato electrónico o impreso del Hospital debe estar debidamente identificada por el área de calidad con el fin de realizar control documental y cambio de versiones. Con esto se alimenta el inventario y clasificación de los archivos de información.

- Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratistas, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas de información la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

- Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos.

- Los usuarios deben renovar periódicamente su clave de acceso al sistema, esto deben solicitarlo a la oficina de Sistemas de Información quienes le facilitarán el acceso y lo acompañarán en el proceso.

- Está totalmente prohibido*:* El intento o violación de los controles de seguridad establecidos; el uso sin autorización de los activos informáticos; el uso no autorizado o impropio de la conexión al sistema; el uso indebido de las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios, aún con la autorización expresa del usuario propietario de la misma.

- El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas de Información.

- Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario. Si detectan actividades irregulares con su código, deben solicitar una auditoría a la oficina de Sistemas de Información que se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informara qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).

- Informar inmediatamente a la oficina de Sistemas de Información cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intentar distribuir este tipo de información interna o externamente.

- A cualquier infracción a la política de sistema de gestión de la seguridad de la información cometida por un funcionario y/o contratista de la ESE Hospital San José del Guaviare, se informará al área de control interno de gestión para que se realice el debido proceso.

- En caso de presentarse un problema crítico a nivel informático en horario no laboral afectando el normal funcionamiento de la institución, la oficina de Sistemas de Información dispone de un funcionario para atender y solucionar estos inconvenientes que está debidamente reportado en el cuadro de disponibilidades.

- Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, uso de proxys, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas.

- Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información es crítica.

- La oficina de Sistemas de Información es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la institución.

- Los usuarios de la red de la ESE Hospital San José del Guaviare recibirán capacitación para el manejo de las herramientas desarrolladas en la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Está totalmente prohibido el uso de contraseñas o claves de otro usuario.

- Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad, que permita al Hospital proteger la información.

SEGURIDAD DEL SOFTWARE

- La oficina de Sistemas de Información es la única responsable de la instalación de software informático y de telecomunicaciones.

- En los equipos de cómputo de la ESE Hospital San José del Guaviare, no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de “Cracks”, “Keygens” y demás aplicativos.

- Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la institución.

- Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

- Las medidas de protección lógica (a nivel de software) son responsabilidad del personal de sistemas de información y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Sistemas de Información.

- La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas de Información y a la disponibilidad presupuestal con el que se cuente.

- Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar apoyo a la oficina de sistemas de información quien asignara una carpeta de Red enrutada al almacenamiento conectado en Red (NAS) y un usuario y contraseña con el cual accederán a la carpeta y guardaran la información que desean preservar. La información que no correspondan a la entidad como fotos, música, etc, será borrada sin previo aviso de la NAS.

- La oficina de Sistemas de Información administrará los diferentes tipos de licencias de software con la que cuenta la ESE Hospital San José del Guaviare y vigilará su vigencia de acuerdo a sus fechas de caducidad.

- La oficina de sistemas de información debe ser notificada inmediatamente por el líder del proceso, cuando un funcionario, contratista o tercero a quien se le haya asignado usuario y contraseña para el manejo del software institucional, se encuentre desvinculado laboralmente de la entidad.

SEGURIDAD DE LAS REDES E INTERNET

- Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de Información de la ESE Hospital San José del Guaviare previa solicitud.

- Se prohíbe utilizar la red y los equipos de institución para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

- En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la institución.

- Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas de Información establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

- Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.
- Utilizar los recursos de la institución para el acceso no autorizado a redes y sistemas remotos.
- Acceder remotamente a los equipos de la institución, los únicos funcionarios autorizados para realizar estas prácticas son los de la oficina de Sistemas de Información, al momento de dar soporte a los usuarios en horario extra laboral o aquellos que se encuentren en modalidad de teletrabajo, previa autorización de la oficina de sistemas de la información.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.
- Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.
- Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.
- Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.
- El intercambio no autorizado de información de propiedad del Hospital, de sus usuarios y/o sus funcionarios, con terceros.

- ❖ El acceso a cuentas de correos personales de ningún tipo desde la red del Hospital y solo se podrán utilizar las cuentas de correo electrónico suministradas por la Institución.
- ❖ Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario.

- La oficina de sistemas realizará monitoreo permanente de tiempos de navegación y actividades realizadas a páginas vistas por parte de los funcionarios y/o contratistas.

- Los servicios bancarios vía web a nombre de la ESE Hospital San José del Guaviare, solamente podrán ser utilizados por el jefe de tesorería y únicamente en el equipo que este tenga asignado. La oficina de Sistemas de Información, tendrá habilitado otro equipo para esta tarea a fin de dar apoyo y soporte cuando se solicite.

- El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido únicamente por la oficina de Sistemas de Información.

- Los mensajes y la información contenida en los buzones de correo son de propiedad de la Hospital San José del Guaviare.

SEGURIDAD DE LOS DATOS E INFORMACIÓN

La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

- Toda información de la ESE Hospital San José del Guaviare generada con los diferentes programas computacionales (Word, Project, Access, Excel, etc.), que requiera ser enviada fuera de la entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de Sistemas. La información puede ser

enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la institución y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

- El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.

- Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado por la normatividad vigente (gestión documental y archivo de historias clínicas), por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva.

- La copia de seguridad de la base de datos central de la ESE Hospital San José del Guaviare se genera así: Tres copias diarias y almacenadas externamente en el servidor de almacenamiento conectado en Red (NAS); al generar la última copia del día se eliminarán las dos anteriores con el fin de no ocupar espacio innecesario de almacenamiento. Estas copias deben ser monitoreadas a diario con el objetivo de garantizar la correcta realización y funcionamiento de las mismas. La ubicación de los medios de almacenamiento, deberá estar alejada del polvo, humedad o cualquier contacto con material que produzca corrosión.

- Cualquier aplicación, archivo desconocido, sospechoso o que contenga extensiones poco comunes en la entidad como .exe que aparezca en la información del usuario (ya sea en el equipo local, correo electrónico), no debe ser abierto o ejecutado sin antes contar con la asesoría de la oficina de Sistemas de Información, que se encargará de examinar y determinar si la aplicación o archivo es potencialmente peligrosa para el equipo o la red de la entidad.

- No está permitido extraer información por ningún medio y bajo ningún motivo de la institución.

- Atender todas las disposiciones de la Ley 527 de 1999. Que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

- Atender las disposiciones de La Ley 594 del 2000, “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.” y lo establecido en la política institucional de gestión documental.

ADMINISTRACIÓN DE SEGURIDAD INFORMÁTICA

- El nivel de prioridad de cada servicio en cuanto a seguridad y estabilidad informática, deberán estar bajo monitoreo permanente y se define en el siguiente orden:

ASISTENCIALES	
1	SERVICIO DE URGENCIAS
2	SERVICIO DE QUIROFANOS
3	SERVICIO DE HOSPITALIZACION
4	SERVICIO DE CONSULTA EXTERNA
5	SERVICIO DE APOYO DIAGNOSTICO Y TERAPEUTICO

ADMINISTRACION	
1	SISTEMAS DE INFORMACION
2	ARCHIVO CLINICO
3	FINANCIERA
4	RECAUDO
5	ARCHIVO Y CORRESPONDENCIA
6	OTROS

- Las auditorías de uso de los recursos informáticos a cada dependencia de la ESE Hospital San José del Guaviare deberán realizarse periódicamente de acuerdo al calendario que establezca la Oficina de sistemas de información.

- Los hallazgos encontrados serán reportados a la oficina de Control Interno, Calidad y Gerencia para que se establezcan los correctivos necesarios.

- Los líderes de oficina son los responsables en la implementación y garantía inicial del cumplimiento de los lineamientos que hayan sido publicadas, modificadas o adicionadas recientemente. Cualquier violación a la política y normas de seguridad establecidas en este documento y aprobadas mediante acto administrativo será sancionada.

ACUERDOS SOBRE CONFIDENCIALIDAD

- Todos los funcionarios, colaboradores y/o terceros que presten sus servicios a la ESE Hospital San José del Guaviare deberán aceptar los acuerdos de confidencialidad definidos por la institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

- Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la institución a personas o entidades externas.

- Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

CONTROLES DE ACCESO FÍSICO

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

- De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

- Los funcionarios, contratistas y terceros de la ESE Hospital San José del Guaviare, así como los visitantes, deben portar su identificación y/o carnet de manera visible durante el tiempo que permanezca dentro de las instalaciones de la organización.

- Los privilegios de acceso a las áreas seguras y restringidas de la institución deben ser periódicamente revisados, actualizados y monitoreados.

RIESGOS EN EL MANEJO DE LA INFORMACIÓN

1. Perdida o alteración de información.
2. Filtración de datos confidenciales de los usuarios de la entidad.
3. Filtración de datos privados de la entidad.
4. Usurpación de identidad ante los aplicativos utilizados.

PLANES DE CONTINGENCIA

Los planes de contingencia se realizarán de acuerdo a los establecido en el manual general de mantenimiento**.**

b. RESPONSABLES

Es responsabilidad de TODOS los funcionarios y colaboradores dar cumplimiento a la POLITICA DE SISTEMA DE GESTIÓN DE LA INFORMACIÓN.

c. INDICADORES

1. CUMPLIMIENTO DEL PLAN DE CAPACITACIONES DE LA POLITICA

Numero de capacitaciones realizadas en el periodo de medición
_____x100
Total, de capacitaciones programas en el periodo de medición

2.

2. SEGUIMIENTO Y EVALUACIÓN

Recolección, análisis y monitoreo de datos para comprobar el cumplimiento y avance según objetivos propuestos, para luego mejorar y/o fortalecer las debilidades y no conformidades identificadas.

3. BIBLIOGRAFIA

9. CONTROL DE REVISIONES Y CAMBIOS DEL DOCUMENTO

ELABORÓ	REVISO	APROBO
NOMBRE CARGO	NOMBRE CARGO	NOMBRE CARGO

VERSION	FECHA DE REVISION O ACTUALIZACION	DESCRIPCION GENERAL DEL CAMBIO REALIZADO

10. ANEXO TECNICO

Debe contener todos los formatos e instrumentos soportes que operativizan la política

file:///C:/Users/Windows-7/Pictures/Downloads/12.%20Plan%20%20de%20seguridad%20y%20privacidad%20de%20la%20informacion.pdf
https://hospitalquindio.gov.co/hospital/documentos/PoliticasDeSeguridad/politicas_seguridad.pdf

https://www.hpshospitales.com/declaracion-de-privacidad-2/

https://www.hospitalubate.gov.co/MANUAL%20DE%20POLITICAS%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf

https://ese-hospital-nuestra-senora-de-las-mercedes-1.micolombiadigital.gov.co/sites/ese-hospital-nuestra-senora-de-las-mercedes-1/content/files/000005/210_manual-politicas-de-seguridad-de-la-informacion.pdf

-