POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 1000-21-001
	Versión: 4
	Fecha de actualización: 26/Jun/2019

1. DECLARACIÓN DEL COMPROMISO

La **ESE Hospital del Sur "G.J.P."** propende por la protección de la información física y electrónica que almacena, recolecta, produce y gestiona a través de la implementación de controles físicos y lógicos, gestión de riesgos y la mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

La Política de Seguridad y Privacidad de la Información aplica a todos los niveles de la organización, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros, que en razón del cumplimiento de sus funciones y las de la ESE Hospital del Sur "G.J.P." compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

La presente política se fundamenta en los siguientes principios:

1. La información es uno de los activos más importantes de la ESE Hospital del Sur "G.J.P." y por lo tanto se espera que sea utilizada acorde con los requerimientos de sus funciones.

2. Confidencialidad, la información de la ESE Hospital del Sur "G.J.P." y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre y que sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones.

3. Integridad, la información de la ESE Hospital del Sur "G.J.P." debe preservar su integridad independientemente de su residencia temporal o permanente, o la forma en que sea transmitida y que esté protegida contra modificaciones no planeadas, realizadas con o sin intención.

4. Disponibilidad, la información de la entidad debe estar disponible cuando sea requerida.

5. Privacidad, la información debe ser preservada y que sea utilizada para los propósitos que fue obtenida.

2. MARCO LEGAL

- Que en el **Artículo 15 de la Constitución Política de Colombia** se establece que: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas".

- **LEY 1266 DE 2008:** "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales,

en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

- **LEY 1273 DE 2009:** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- **LEY 1581 DE 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales tiene como objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

- **LEY 1712 DE 2014:** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública".

- **Decreto 1078 de 2015:** "Se expidió el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones."

- **Que el Decreto 1078 de 2015:** dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

- **DECRETO 1008 DE 2018:** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones."

3. PROPÓSITO

Promover el uso de tecnologías de Información y Comunicación – TIC en entornos seguros, mediante normas simples aplicables al usuario del sistema de información, apoyado mediante herramientas que permitan prestar servicios de salud eficientes y confiable.

4. LINEAMIENTOS ESTRATÉGICOS DE LA POLÍTICA

A partir del Modelo de Seguridad y Privacidad de la Información emanado por el **Ministerio de Tecnologías de la Información y las comunicaciones - MINTIC**, La **ESE Hospital del Sur "G.J.P."** declara:

a. La ESE Hospital del Sur "G.J.P." establece los roles y responsabilidades relacionados con la presente política de seguridad y privacidad de la información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.

b. La entidad protege la información producida, custodiada y transmitida en desarrollo de sus procesos misionales.

c. El proceso de Gerencia de Información, diseñará e implementará la estrategia para proteger la información generada, recolectada, procesada y utilizada en el cumplimiento de la misión de la Entidad.

d. El proceso de Gerencia de Información establecerá los lineamientos para la identificación, clasificación y buen uso de los activos de información físicos y digitales, para su protección.

f. Si bien el proceso de Gerencia de Información suministra y gestiona las herramientas de hardware y software para el procesamiento y almacenamiento de la información y a su vez implementa controles para mitigar los riesgos sobre dicha información; los propietarios de la información son los responsables de los procesos institucionales y por ende de la información registrada, de la autorización de cambios y la solicitud de modificaciones a realizar sobre los sistemas de información o su información.

g. Las dependencias de la ESE Hospital del sur "G.J.P." que tienen la custodia de la información generada en el marco de sus funciones deben aplicar los controles correspondientes para proteger la información y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.

h. Los activos de información, equipos, bienes, aplicaciones, herramientas tecnológicas y servicios de Tecnologías de la Información y las Comunicaciones en adelante TIC, asignadas por el Hospital son para uso exclusivo del cumplimiento de las funciones designadas; razón por la cual la información almacenada, procesada y generada a través de dichos activos, herramientas y dispositivos se considera propiedad de la entidad y el uso inadecuado de dichos recursos puede conllevar a sanciones disciplinarias y legales correspondientes.

i. Es obligación de todos los funcionarios, contratistas y proveedores adscritos a la ESE Hospital del Sur "G.J.P." cumplir con la **"Política de Seguridad y Privacidad de la Información"** Y propender por la integridad, disponibilidad y confidencialidad de la misma, so pena de que la entidad tome las medidas disciplinarias, legales y administrativas correspondientes.

j. Teniendo en cuenta que todos los activos de información deben tener un responsable, la creación de cuentas de usuario y/o correo electrónico genéricos (que no estén asociados a un funcionario o contratista) no estarán autorizadas.

k. Es responsabilidad de los funcionarios y contratistas de la ESE Hospital del Sur "G.J.P." solicitar copias de seguridad de los archivos más sensibles que se almacenan en los equipos de cómputo asignados; esta copia debe almacenarse en los medios designados por la ESE tales como servidor de archivos, almacenamiento en Disco externos, entre otros. Una vez finalizada la vinculación con la entidad se deberá entregar toda la información procesada dentro de los equipos a cargo al jefe inmediato o al supervisor de contrato.

En términos generales la política de seguridad y privacidad de la información, engloba los procedimientos más adecuados para la Gerencia de la información en los diferentes

niveles de la organización, tomando como lineamientos principales cuatro criterios, los cuales están soportados en:

- Seguridad Organizacional.
- Seguridad Física y Lógica.
- Seguridad Legal.

4.1. SEGURIDAD ORGANIZACIONAL

Dentro de ésta, se establece el marco formal de seguridad que tiene la institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

4. 1. 1. Gestión del Recurso Humano

La ESE Hospital del Sur "G.J.P." a través de los Procesos de Gerencia del Talento Humano y Gerencia de Información son los responsables de divulgar la Política de Seguridad y Privacidad de la Información a todos los funcionarios o contratistas que se vinculen a la entidad.

El área Jurídica y de contratación deben realizar las tareas pertinentes para que todos los contratos de prestación de servicios, incorporen las obligaciones correspondientes a exigir el cumplimiento de la Política de Seguridad y Privacidad de la Información, el manejo confidencial de la información, la cesión de derecho de autor a la entidad y la protección de datos.

Cuando un funcionario o contratista cese en sus funciones o culmine la ejecución de un contrato en la ESE Hospital del Sur "G.J.P.", el jefe inmediato o supervisor del contrato será el encargado de la custodia de los recursos de información.

4. 1. 2. Activos de Información

La ESE Hospital del Sur "G.J.P." a través del Proceso de Gerencia de Información, debe establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información físicos y digitales, con el objetivo de garantizar su protección.
Inventario y propiedad de los activos: La responsabilidad de la administración, gestión e implementación de controles de los activos de información está en cabeza del propietario de los mismos. Los activos de Información de la ESE deben ser identificados, clasificados y controlados para propender su uso adecuado, protección y la recuperación ante cualquier desastre.
Los propietarios de la información deben propender para que los custodios mantengan actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez por año. La consolidación de dicho inventario está bajo la responsabilidad del proceso de Gerencia de Información y Gestión Documental.

Con el objeto de implementar los controles de seguridad, las dependencias que tienen la custodia de la información en el marco de su función, se encargaran de proteger la información, mantener y actualizar el inventario de activos.

4. 1. 3. Archivos de Gestión

El área de Gestión Documental, debe implementar controles para garantizar que los archivos de gestión de la entidad cuenten con los mecanismos de seguridad que salvaguarden y conserven dicha información. En este sentido, es importante resaltar lo preceptuado el **Artículo 15 de la Ley 594 de 2000**": *Los servidores públicos, al desvincularse de las funciones titulares, entregarán los documentos y archivos a su cargo debidamente inventariados, conforme a las normas y procedimientos que establezca el Archivo General de la Nación, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades.*

4. 1. 4. Clasificación de la Información

Los propietarios de los activos de información deben documentar la clasificación de seguridad de los activos de los que son responsables y designarán un custodio para cada activo a su vez éste será responsable de la implementación de los controles de seguridad.

La clasificación de la información de la ESE Hospital del sur "G.J.P." se debe realizar con base en la **ley 1712 de 2014** reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del **Decreto 1081 de 2015** y la **ley 594 de 2000 (Ley General de Archivos)**.

Uso Aceptable de los Activos: Los recursos tecnológicos al igual que los archivos, carpetas, bases de datos, aplicaciones y documentos, son activos de información que pertenecen a la ESE Hospital del sur "G.J.P." , por lo cual su uso es exclusivamente institucional y es responsabilidad de aquel a quien se asigne o corresponda su uso, el propender por su confidencialidad, integridad, disponibilidad, privacidad y buen uso, estos son:

A. Correo Electrónico

El correo electrónico institucional asignado es un servicio para la comunicación y colaboración de los funcionarios y contratistas de la ESE Hospital del Sur "G.J.P.", de uso personal e intransferible, que debe utilizarse responsablemente cumpliendo como mínimo con los siguientes lineamientos:

- El correo electrónico es de uso exclusivo, para los empleados de la ESE Hospital del Sur "G.J.P." y para manejo de información interna, por ello la entidad está facultada para revisar las cuentas de los empleados con autorización de la gerencia cuando la situación lo amerite.
- El correo electrónico asignado debe ser para uso única y exclusivamente institucional y no podrá ser utilizado para fines personales, económicos, comerciales, propaganda, campañas, invitaciones y cualquier otro ajeno a los propósitos de la entidad.
- Los Funcionarios deben garantizar que su cuenta de correo se encuentra depurada, es decir, sin correos con antigüedad mayor de un mes o con un tamaño mayor de 100 MB. De lo contrario el administrador del sistema podrá eliminar sin autorización previa dichos correos y el empleado se hará acreedor a un llamado de atención
- Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación temporal o total de la cuenta dentro del sistema.
- La cuenta de correo institucional no podrá ser utilizada para el registro o autenticación, en páginas o sitios publicitarios, de comercio electrónico, deportivos, redes sociales, casinos, concursos, sitios de citas o cualquier otro ajeno a las funciones que le correspondan en la Entidad.

- Está expresamente prohibido distribuir información de la ESE Hospital del Sur "G.J.P." que no sea considerada de uso público a otras entidades o ciudadanos, sin la debida autorización de dueño del activo de información.
- El usuario será responsable de la información que sea enviada con su cuenta y de la información que se descargue en los equipos de la ESE desde ella.
- Está prohibido el envío de correos masivos tanto internos como externos.
- Los correos electrónicos catalogados tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deberán reportar al área de Sistemas de Información a través de la mesa de ayuda y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM.
- No se deben abrir correos desconocidos, en otros idiomas o con mensajes incoherentes por el riesgo de virus.
- Se deben enviar los correos de acuerdo a los lineamientos generales dados en el Manual para la elaboración de comunicaciones oficiales.
- El correo electrónico debe ser revisado por los funcionarios por lo menos dos (2) veces al día, no realizarlo no lo exime de la responsabilidad de conocer la información suministrada por este medio.
- El área de informática emplea dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

B. Internet:

Si bien desde el proceso de Gerencia de información se establecen controles a la navegación de acuerdo a las políticas y perfiles establecidos, es responsabilidad de todos los funcionarios y contratistas de la ESE hacer un uso responsable del Internet y cumplir con las políticas para tal fin aquí establecidas:
La ESE Hospital del Sur "G.J.P.", en cabeza del proceso de Gerencia de Información, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.

- La ESE Hospital del Sur "G.J.P.", a través del proceso de Gerencia de Información, se reserva el derecho de monitorear, hacer seguimiento y auditoría al uso que los usuarios le den, para verificar que se haga un uso responsable y racional de dicho recurso.
- El uso del Internet deberá ajustarse a las necesidades de la función u obligaciones contractuales dentro del marco institucional y se prohíbe expresamente el acceso o consulta de páginas Web con contenido insultante, ofensivo, injurioso, obsceno, pornográfico, violatorio de los derechos de autor y todo aquel que atente contra la integridad moral.
- El acceso a sitios Web o la instalación de aplicaciones para intentar evadir los controles y políticas de seguridad de navegación está totalmente prohibidos y su detección será tratada como un incidente de seguridad.
- El bajar archivos provenientes de Internet implica un riesgo para la seguridad de la información, así como un riesgo de infracción al régimen legal de derechos de autor, por lo cual se solicita que únicamente se haga cuando sea necesario; está prohibido la descarga de archivos con extensiones de tipo .exe, .bat, .prg, .bak, .piq.

C. Equipos de cómputo y otros Dispositivos

La ESE Hospital del Sur "G.J.P." podrá asignar a los funcionarios y contratistas computadores de escritorio, portátiles, Tablet, teléfonos IP, teléfonos inteligentes o dispositivos similares para el desarrollo de sus labores; el manejo de dichos equipos

por parte de éstos, conlleva responsabilidades y deben ajustarse a las siguientes directrices generales:

- Aquellos dispositivos que requieran clave de acceso, dicha clave es de uso personal y no podrá ser compartida, razón por la cual la responsabilidad de un posible mal uso recaerá sobre el funcionario o contratista a quien se asignó dicho usuario y clave.
- Los dispositivos asignados solo podrán usarse para fines laborales relacionados con las funciones y obligaciones designadas, razón por la cual no hay autorización de instalar software diferente al autorizado por la Entidad.
- Los dispositivos de cómputo y móviles que sean asignados a los funcionarios y contratistas, serán para uso institucional exclusivamente e intransferibles y la responsabilidad de su uso recaerá sobre la persona a la que le fue asignado.
- Teniendo en cuenta que los equipos son para uso institucional, La ESE Hospital del sur "G.J.P." se reserva el derecho de monitorear el contenido y software instalado en los equipos de la entidad para verificar el tipo de información, su uso y licenciamiento del software instalado. De esta manera contenidos de música, vídeo, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del funcionario o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento, será desinstalado.
- Los únicos autorizados para la instalación de software adicional a las aplicaciones base es el personal del proceso de gerencia de información, previa solicitud a través de la mesa de ayuda y luego de la aprobación respectiva (se debe constatar la necesidad de su uso y que la entidad cuente con el respectivo licenciamiento).
- Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, son los funcionarios del área de Gerencia de Información designados previa solicitud a través de la mesa de servicio.
- Es responsabilidad de los funcionarios y contratistas de la ESE mantener organizada la información y solicitar copias de seguridad de la misma contenida en sus estaciones de trabajo y entregarlas en custodia al jefe inmediato o supervisor del contrato al finalizar la vinculación con la Entidad.
- De acuerdo a la política de consumo de tabaco y sustancias alucinógenas está prohibido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos tales como computadores de escritorio, portátiles entre otros.

- El proceso de gerencia de Información encabeza el equipo de mesa de servicio deberá aprovisionar los computadores antes de ser entregados, garantizando que:
- Sean formateados a bajo nivel para que la información de los anteriores usuarios no sea recuperable o accesible.
- El software instalado sea el software base definido por la entidad y que cuente con el respectivo licenciamiento.
- Los sistemas operativos y demás aplicativos tengan instaladas las últimas actualizaciones liberadas a la fecha de entrega del equipo.
- El antivirus este actualizado, funcionando y administrado desde consola.
- Los equipos deberán quedar apagados cada vez que el funcionario o contratista finalice la Jornada laboral, por seguridad y ahorro de energía entre otras.
- Se debe apagar la pantalla cuando se deje de utilizar el equipo por espacios mayores de 15 minutos.
- La ubicación de los equipos de cómputo y el soporte esta priorizado de acuerdo a las jerarquías definidas en la **Matriz de Criticidad**

d. Cableado Estructurado:

En las sedes donde haya cableado estructurado, las tomas eléctricas ubicadas en las

canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas de color naranja y bajo ninguna circunstancia se puede conectar otros elementos en dichas tomas.

En los puntos de red de los usuarios no está permitido realizar conexiones de switches, hub, acces point u otros dispositivos para realizar derivaciones, ni se permite realizar conexiones o derivaciones eléctricas que pongan en riesgo la seguridad física por fallas en el suministro eléctrico.

e. <u>Sistemas de Información:</u> Las credenciales de acceso a la red y a recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas de la ESE Hospital del Sur "G.J.P." no deben revelar éstas a terceros ni utilizar claves ajenas. Todo funcionario y contratista será responsable del cambio de clave de acceso a los sistemas información o recursos informáticos periódicamente.

Cuando se presenten ausencias de funcionarios o contratistas por incapacidades, licencias no remuneradas o suspensión de contrato, será bloqueado el acceso a los Sistemas de Información, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. Es responsabilidad del área de gerencia del talento humano notificar este evento con una solicitud al área de Sistemas.

Solo podrán publicarse aquellas aplicaciones o sistemas de información que deban ser consultados por Personal de la ESE; las demás aplicaciones son de uso interno y su acceso desde fuera de la entidad se debe realizar a través de conexiones seguras con previa autorización por parte del proceso de gerencia de Información.

Ademas se tiene definido y estructurado el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

La creación de perfiles es necesaria para los aplicativos que soportan el sistema de información y que son operados por funcionarios de la entidad

Los perfiles para la ESE están definidos en dos grandes grupos **<u>ASISTENCIAL</u>** y **<u>ADMINISTRATIVOS</u>**

- El perfil asistencial es para los integrantes del equipo de salud, quienes tienen acceso a la información clínica de los usuarios en el software, información que es necesaria para el desarrollo de sus labores.

- El perfil administrativo esta definidos de acuerdo a la funciones financieras y administrativa que realicen los funcionarios responsables de estas labores, no tendrán acceso a la historia clínica del paciente.

El alcance de cada perfil es definido por los líderes de cada proceso, los cuales son parametrizados y revisados con el apoyo del administrador del sistema, al igual que el mantenimiento de los permisos funcionales del sistema generando en cada ajuste un acta que evidencie los cambios realizados.

El administrador del sistema en forma conjunta con los responsables de los servicios, documenta y enviar los requerimientos del software a los respectivos proveedores de software, el administrador del sistema los consolida a través de una matriz de requerimientos, por medio de la cual se realiza seguimiento trimestral para verificar el avance en la resolución de cada uno.

4.2. SEGURIDAD FÍSICA Y LÓGICA

Identifica los límites mínimos que se deben cumplir en cuanto a parámetros de seguridad física y lógica, de forma que se puedan establecer controles de acceso, definición de roles y responsabilidades, perfiles de seguridad, gestión de Incidentes, documentación sobre sistemas de Información, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y adquisición de sistemas.

4. 2. 1. Controles y Seguridad de la Información

Control de Acceso: La ESE Hospital del Sur "G.J.P." a través del proceso de Gerencia de Información y Gestión Documental, propende por implementar controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la entidad. La ESE Hospital del Sur "G.J.P." a través del área Jurídica y Contractual y Gestión del Talento Humano deben establecer los mecanismos para comunicar al proceso de Gerencia de Información las novedades de ingreso y retiro de los funcionarios y contratistas de la ESE, para gestionar los derechos de acceso a los sistemas de información, recursos y servicios tecnológicos de la entidad.

El proceso de Gerencia de Información debe implementar controles, procedimientos e instructivos para proveer el acceso físico y lógico de los recursos informáticos a usuarios autorizados para el cumplimiento de sus funciones estos serán los siguientes:

A. Seguridad Física y del Entorno: La ESE Hospital del Sur "G.J.P.", debe implementar controles para proteger el perímetro de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructuras de soporte a los sistemas de información y comunicaciones.), además mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de la entidad.

Para tal fin se restringe el acceso a las dependencias de sistemas, archivo central, archivo clínico, tesorería y nómina, al personal no autorizado, con el fin de salvaguardar la información que allí se gestiona; Las puertas de acceso a dichas dependencias deben permanecer cerradas.

Además se deben tener cuenta las siguientes consideraciones:

- Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones de la ESE, deberán estar debidamente identificados, con un documento que acredite su tipo de vinculación el cual se deberá portar en un lugar visible.
- No debe existir sobre el escritorio información confidencial o de importancia para la organización a la vista de cualquier persona, ni referencias sobre los códigos de acceso de la persona encargada de algún cargo que sea parte de la organización.

B. Seguridad de las Operaciones:

La ESE Hospital del Sur "G.J.P." a través del Proceso de Gerencia de la Información se encarga de la operación y administración de los recursos tecnológicos que soportan la operación de la entidad y propende por la implementación de los controles asociados a éstos para mitigar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información; para este fin debe cumplir con los siguientes lineamientos:

- Implementar un plan de copias de seguridad que le permita proteger la información crítica alojada en el Data Center de la entidad y su recuperación en caso de desastre.
- Implementar controles para mitigar los riesgos inherentes a códigos maliciosos, sin embargo, los usuarios no pueden instalar software en los equipos de propiedad de la Entidad.
- Implementar un procedimiento para el análisis e introducción de nuevas Tecnologías donde los cambios en la configuración de los equipos, redes, sistemas de información, bases de datos, aplicaciones o cualquier activo de información de Tecnologías de Información-TI sean revisados, evaluados y aprobados.
- Implementar controles para auditar el acceso y uso de datos a los sistemas de información designados por el Proceso de Gerencia de Información para el control de los funcionarios y contratistas, adicionalmente se reserva el derecho de monitorear la actividad donde se sospecha que se ha producido o pueda producir una violación de la política, asegurando el debido proceso y el respeto por los derechos de las partes involucradas.
- Proveer los recursos necesarios para la implementar controles requeridos para la seguridad de las operaciones.

C. Seguridad de las Comunicaciones: La ESE Hospital del Sur "G.J.P." a través del Proceso de Gerencia de la Información establecerá los Acuerdos de Niveles de Servicios-ANS requeridos para que el proveedor de servicios de tecnologías de Información-TI garantice la disponibilidad de las redes WAN e Internet.
La ESE Hospital del Sur "G.J.P." a través del Proceso de Gerencia de la Información debe implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos de la entidad propendiendo la integridad y confidencialidad de la información.

D. Controles en las relaciones con los Proveedores: La ESE Hospital del Sur "G.J.P." a través del Proceso de Gerencia de la Información en colaboración con el área Jurídica y de Contratación, definirán mecanismos de control que aseguren que la información a la que tenga acceso un tercero, cuente con un nivel de protección adecuado y que éstos cumplan con las políticas y procedimientos de seguridad de la información establecidos.

E. Seguridad en la Gestión de Continuidad del Negocio: La ESE Hospital del Sur "G.J.P." en armonía con todos sus procesos deberá implementar los planes de continuidad de negocio y de recuperación de desastres para mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los sistemas de información misionales que sean considerados críticos para la continuación de la operación de la entidad de manera aceptable. La ESE destinará los recursos financieros suficientes para proporcionar una respuesta efectiva de TI, para soportar los procesos claves de la entidad en caso de contingencia o eventos catastróficos que afecten la continuidad de su operación.

F. Gestión de Incidentes de Seguridad de la Información: La ESE Hospital del Sur "G.J.P.", a través del Proceso de Gerencia de la Información se encarga de definir, documentar, mantener, publicar y aplicar los procedimientos para atender, valorar, clasificar y dar respuesta a los eventos de seguridad de la información. De igual forma el proceso de Gerencia de Información deberá promover el reporte de eventos de seguridad de la información para reducir la probabilidad e impacto del riesgo inherente a ellos.

G. Responsabilidades del Usuario:

Las contraseñas son de uso personal e intransferible, cada usuario es responsable exclusivo de mantener a salvo su contraseña, para ello debe:

- Evitar guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.
- Se debe reportar al área de sistemas, los archivos en los cuales se almacene información concerniente al desarrollo de los procesos institucionales y que se encuentre protegida mediante contraseñas, de tal forma que se guarde allí un respaldo de la contraseña y disminuir así el riesgo de pérdida de información por pérdida u olvido de la misma.
- Realizar el cambio de su contraseña como mínimo cada tres meses o cuando sospeche de alguna violación.
- Al dejar el puesto de trabajo, aunque sea por un momento, se deben cerrar las aplicaciones que se estén utilizando.

5. SEGURIDAD LEGAL

Integra los requerimientos de seguridad que deben cumplir todos los funcionarios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación y contrataciones externas.

5.1. Licenciamiento de Software

- Todo el software comercial que utiliza la Institución, se encuentra legalmente registrado, con sus respectivas licencias.
- La adquisición de software por parte de personal que labore en la institución, no expresa el consentimiento de la institución, por ende la institución no se hace responsable de las actividades de sus empleados.
- El software comercial licenciado a la E.S.E es propiedad exclusiva de la institución, la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.
- Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y con base en las disposiciones de la respectiva licencia.
- El software desarrollado internamente, por el personal que labora en la institución es propiedad exclusiva de la institución
- La adquisición del software libre o comercial es gestionado con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtiene software de forma fraudulenta.
- Los contratos con terceros, en la gestión o prestación de un servicio, deben especificar, las medidas necesarias de seguridad, nivel de prestación del servicio, y/o

el personal involucrado en tal proceso cuando se utiliza el sistema de información institucional.

- La instalación de software y hardware se realiza exclusivamente por parte del personal de sistemas.

6. INDICADORES PARA EVALUACIÓN DE LA POLÍTICA

- **Indice de Cumplimiento de la Política de Seguridad y Privacidad de la Información >= 90%**

7. ANEXOS

La evaluación de la política de seguridad del paciente se realiza a través de:

- PATRULLAJE SEGURIDAD INFORMACION

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	08/Abr/2011	Se complementa la política con lo referente a la matriz de criticidad, rondas de seguridad de la información y cronograma de copias de seguridad.
2	02/May/2014	Es importante referenciar que la version 2 de este documento se diseño teniendo en cuenta los nuevos estandares del Sistema único de habilitación, Resolución 1441 de 2013 y del Sistema único de acreditación Resolución 123 de 2012
3	25/Ago/2015	se actualiza política y cambio de formato de patrullaje de seguridad.
4	15/May/2019	Se actualiza política de acuerdo a los lineamientos del Modelos de Seguridad y Privacidad de la Información - MSPI de MinTIC.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Responsable Gerencia de la Información **Cargo:** Profesional Universitario Ingeniero de Sistemas **Fecha:** 25/Abr/2019	**Nombre:** Lider de calidad **Cargo:** Líder de Calidad **Fecha:** 26/Jun/2019	**Nombre:** Gerente **Cargo:** Gerente **Fecha:** 26/Jun/2019