TABLA DE CONTENIDO

1. INTRODUCCIÓN

En la actualidad la información de la institución se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos en nuestra institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude digital, espionaje, sabotaje, vandalismo, fuego, robo e inundación y ciberataques. La posibilidad de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio (DoS) se hacen cada vez más comunes.

Con la promulgación del presente plan de Seguridad de la Información la E.S.E. Hospital San Juan de Dios formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

Este manual describe las políticas, normas, sanciones y reglas en cuanto a la gestión de la seguridad de la información como documento para consulta de todos los interesados (usuarios, funcionarios, contratistas, terceros, etc.) y está basado en la norma NTC-ISO-IEC 27001:2013.

De esta manera, la Seguridad de la Información es una prioridad para la E.S.E Hospital San Juan de Dios de Yarumal y por tanto es responsabilidad de todas las partes interesadas cumplir con el presente manual y velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de las políticas contenidas en dicho documento.

Objetivo general

Crear un plan de gestión que garantice la seguridad y privacidad de la información. Este plan estará diseñado para minimizar los riesgos asociados a la pérdida de activos de información y para mantenerlos en un entorno razonablemente seguro, en consonancia con la misión de la ESE Hospital San Juan De Dios de Yarumal. Además, se busca proteger los activos de información y asegurar un uso adecuado de los recursos, así como gestionar los riesgos de manera efectiva. Todo esto con el fin de preservar la disponibilidad, integridad y confidencialidad de la información, y asegurar la continuidad de todos los procesos administrativos y asistenciales.

Objetivos específicos

- Proteger, preservar y administrar objetivamente la información de la E.S.E. junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
- Mantener el plan de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la E.S.E. para asegurar su permanencia y nivel de eficacia.
- Definir las directrices de la ESE Hospital San Juan de Dios para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.
- Establecer los roles y las responsabilidades referentes al cumplimiento de la seguridad de la información.
- Gestionar los riesgos asociados a la seguridad de la información es fundamental para mantenerlos dentro de niveles aceptables. Es importante sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas sobre el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información del Gobierno en Línea. De este modo, se busca fortalecer la conciencia sobre la necesidad de proteger los proteger los activos de información institucionales.

Alcance

Este plan es de aplicación en el conjunto de dependencias que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la E.S.E. a través de contratos o acuerdos con terceros y a todo el personal de la E.S.E. Hospital San Juan de Dios, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Este documento es de obligatoria aplicación para todos los funcionarios de la E.S.E Hospital San Juan de Dios. Así mismo, proveedores y personal externo que desempeñen labores o proporcionen algún tipo de servicio o producto a la institución, estarán obligado a cumplir con el plan aquí descrita.

2. QUE ES LA SEGURIDAD DE LA INFORMACIÓN

Es un conjunto de prácticas, políticas y tecnologías diseñadas para proteger los datos y sistemas de acceso no autorizado, uso indebido, divulgación, modificación, destrucción o interrupción.

Principios Fundamentales o triada CID

- **Confidencialidad:** Asegurar que la información esté accesible solo para quienes tienen autorización.
- **Integridad:** Garantizar que la información sea precisa y esté protegida contra alteraciones no autorizadas.
- **Disponibilidad:** Asegurar que los datos y sistemas estén accesibles para los usuarios autorizados cuando los necesiten.

Componentes Clave

- **Gestión de riesgos:** Identificar, evaluar y mitigar amenazas potenciales.
- **Control de acceso:** Definir y limitar quién puede acceder a qué recursos.
- **Cifrado:** Proteger los datos mediante algoritmos que convierten la información en un formato ilegible sin la clave correcta.
- **Auditorías y monitoreo:** Supervisar continuamente las actividades para identificar y responder a incidentes.
- **Concienciación:** Educar a los usuarios sobre buenas prácticas de seguridad.
- **Protección a la duplicación:** Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- **No repudio:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- **Legalidad:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.

3. CONTINGENCIA RECUPERACIÓN Y RETORNO A LA NORMALIDAD

Objetivo

Definir las actividades necesarias para llevar a cabo el plan de contingencia, recuperación y retorno a la normalidad de la plataforma de información de la ESE Hospital San Juan De Dios De Yarumal, es esencial en este caso de que ocurra algún desastre ya se natural, ciberataque o de otra índole que interrumpa las operaciones de los recursos informáticos

y/o servicios de la institución.

Alcance

Identificar el tipo de desastre y elaborar un informe final sobre el suceso, donde se evidencie cuáles fueron las causas, los servicios afectados, las acciones que se tomaron y finalmente los resultados obtenidos

Responsabilidades

El área de Tecnología a cargo del líder de sistemas junto con su equipo de trabajo deberá identificar el tipo de desastre que se presentó e informar de manera inmediata a los directivos de la entidad sobre dicho suceso y los daños que se han podido detectar en la evaluación preliminar, se debe definir el tiempo estimado de recuperación ante dicho suceso y elaborar un informe sobre el problema presentado y su solución para una futura retroalimentación.

Las diferentes dependencias de la ESE Hospital San Juan De Dios De Yarumal deberán implementar un plan de contingencia, donde definirán las acciones que se deben ejecutar cuando se presenta dicho desastre, logrando con esto que el servicio se siga prestando mientras el equipo de sistemas completa el proceso de recuperación y restablecimiento del servicio.

Desafíos Actuales

- **Ciberataques**: Phishing, ransomware, ataques de día cero, entre otros**.**
- **Protección de datos en la nube**: Asegurar datos almacenados y procesados en infraestructuras de terceros.
- **IoT (Internet de las Cosas):** Multiplicidad de dispositivos conectados que amplían la superficie de ataque.
- **Ingeniería social**: Manipulación psicológica para obtener información confidencial.

Mejores Prácticas

- Actualizar software regularmente.
- Implementar autenticación multifactor (MFA).

- Realizar respaldos periódicos.
- Clasificar y etiquetar datos sensibles.
- Establecer y probar un plan de respuesta a incidente

4. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

La ESE Hospital San Juan de Dios garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral del presente plan.

Los jefes de dependencia, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsables de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en este plan y en los estándares, normas, guías y procedimientos.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.1 Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

La institución establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

5.2 Responsabilidad

El área de sistemas de la institución es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto del plan de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la

estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicha área definir las estrategias de capacitación en materia de seguridad de la información al interior de la E.S.E.

El Coordinador del área de sistemas y archivo clínico serán los responsables de coordinar las acciones y de impulsar la implementación y cumplimiento del presente plan.

Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El área de talento humano cumplirá la función de notificar a todo el personal que se vincula contractualmente con la E.S.E., de las obligaciones respecto del cumplimiento del plan de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación del presente Plan y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los *Compromisos de Confidencialidad* y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el área de sistemas.

El Área de Jurídico verificará el cumplimiento del presente Plan en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir el plan de Seguridad de la Información vigente.

La Oficina de control interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

6. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN.

Cada dependencia, bajo supervisión del área de sistemas, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Subgerente Administrativo**,** correspondiendo a la oficina de sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El área de sistemas en coordinación con la **Subgerencia Administrativa** y la **Sección de Almacén** tienen la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

7. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal de la E.S.E. Hospital San Juan de Dios, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La oficina de sistemas debe mantener un directorio completo y actualizado de tales perfiles.

El área de sistemas determina cuales son los permisos que deben darse para los diferentes perfiles de los colaboradores de la institución.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

Responsabilidades del personal de la ESE

Todo el personal de la E.S.E. Hospital San Juan de Dios, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acta **AT-20-001 Compromiso de confidencialidad** el cual contiene los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los

lineamientos dados por la oficina de sistemas, en cuanto a la información, equipos y software.

Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de la E.S.E. quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios deben ser creados y mantenido por la oficina de sistemas en conjunto con la oficina de recursos humanos.

Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

8. SEGURIDAD FÍSICA Y DEL ENTORNO

Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. La oficina de sistemas elaborará y mantendrán las normas, controles y registros de acceso a dichas áreas, donde solo el personal de sistemas tiene acceso a dichas áreas y control de ingreso a las mismas.

Seguridad en los equipos

Los servidores que contengan información y servicios institucionales deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la oficina de sistemas. El área de sistemas define el límite de responsabilidades de las dependencias. No se permite el alojamiento de información institucional en servidores externos sin una aprobación por escrito del Gerente de la E.S.E.

Equipos claves de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La oficina de sistemas debe asegurar que la infraestructura de servicios de TI este cubierta por mantenimiento y soporte adecuados de hardware y software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el área de sistemas.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad según protocolo de copias de seguridad PT-20-001.

9. ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

Reporte e investigación de incidentes de seguridad

El personal de la E.S.E debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la oficina de sistemas. En casos especiales dichos reportes podrán realizarse directamente a la Gerencia, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

El área de sistemas debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

En conformidad con la ley, la ESE podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización de la Gerencia, y en todo caso notificando previamente a los afectados por esta decisión.

La oficina de sistemas mantendrá procedimientos escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.

10. PROTECCIÓN, CONFIGURACION Y CUSTODIA

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El área de sistemas elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo de la E.S.E. deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus y también con controlador de dominio. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

La E.S.E. a través de la oficina de sistemas podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

La oficina de sistemas debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo al protocolo documentado por el área de sistemas. dicho protocolo debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de la E.S.E. deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. La oficina de sistemas debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La oficina de control interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Las copias de seguridad de información crítica deben ser mantenidas de acuerdo a cronogramas definidos y publicados por la oficina de sistemas.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y

custodia.

Administración de configuraciones de red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por el área de sistemas.

Todo equipo de TI debe ser revisado, registrado y aprobado por el área de sistemas antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

Intercambio de información con organizaciones externas.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Gerencia de la E.S.E., y dirigida por dichos entes a los responsables de su custodia.

Toda la información institucional debe ser manejada de acuerdo a las políticas institucionales

Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el área de sistemas y en todo caso esta área debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas de la E.S.E. deben ser aprobadas por la oficina de sistemas**,** de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La oficina de sistemas debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde al área de sistemas mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales

11. CONTROL DE ACCESO

Categorías de Acceso

Los accesos a los recursos de tecnologías de información institucionales deben estar restringidos según los perfiles de usuario definidos por el área de sistemas de la E.S.E.

Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

Corresponde al área de sistemas elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal asistencial, administrativo y terceros.

El área de sistemas debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.

La E.S.E. debe procurar mantener al mínimo la cantidad de cuentas de usuario que el personal administrativo, médicos, auxiliares y terceros deban poseer para acceder a los servicios tales como el programa Xenco de sistema de gestión hospitalario entre otros.

El control de las contraseñas de red y uso de equipos es responsabilidad del área de sistemas., dichas contraseñas deben ser encriptadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por el área de sistemas de la E.S.E. y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos al área de sistemas las cuales deben ser conservadas por la subgerencia Administrativa y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

El área de sistemas debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

Como requisito para la terminación de relación contractual o laboral del personal de la E.S.E., el área de sistemas debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la

institución.

Equipos móviles

La E.S.E. reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (portátiles, celulares, tablets, etc). Corresponde a la oficina de recursos humanos en conjunto con la oficina de sistemas elaborar, mantener e implementar planes de capacitación que faciliten la formación y toma de conciencia en cuestiones de seguridad de la información.

Auditoria y Seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en la E.S.E. deben ser seguidos y auditados de acuerdo con los lineamientos del código de ética y del código de uso de recursos de tecnologías de la información, el cual debe ser elaborado por el área de control interno y calidad.

Acceso Remoto

El acceso remoto a servicios de red ofrecidos por la E.S.E. debe estar sujeto a medidas de control definidas por el área de sistemas, las cuales deben incluir acuerdos escritos de seguridad de la información, donde los accesos remotos por fuera del hospital deben estar debidamente aprobados por el jefe del área o en su defecto por uno de los directivos.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS SOFTWARE

Para apoyar los procesos operativos y estratégicos la E.S.E. debe hacer uso intensivo de las tecnologías de la información y las comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

El área de sistemas debe elegir, elaborar, mantener y difundir el “Método de Desarrollo de Sistemas Software en la E.S.E. Hospital San Juan de Dios” que incluya lineamientos, procesos, buenas prácticas, plantillas y demás que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de identificación y valoración de riesgos del proyecto. La E.S.E. no debe emprender procesos de desarrollo o mantenimiento de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

13. CUMPLIMIENTO

Todo uso y seguimiento de uso a los recursos de TI en la E.S.E. Hospital San juan de Dios debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en la materia, incluido, pero no restringido a:

Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
• Ley 23 de 1982. Sobre derechos de autor.
• Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
• Ley 527 de 1999. Por la cual se 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. Ley 594 de 2000. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
• Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas.
• Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
• Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
• 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 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
• Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
• Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
• Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

• Ley 2088 de 2012. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
• Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
• Ley 1753 de 2015. Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país.

- Ley 1755 de 2015.Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

• Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario.

- Decisión Andina 351 de 1993. Régimen común sobre derecho de autor y derechos conexos.
- Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 2609 de 2012.Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de datos.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1081 de 2015.Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 103 de 2015.Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1068 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para

fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

- Decreto 1008 del 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.
- Decreto 612 de 2018.Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Decreto 1287 de 2020.Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 767 de 2022.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.
- Decreto 88 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.

14. TÉRMINOS Y DEFINICIONES

- **Información:** Toda forma de conocimiento objetivo con representación física o lógica explícita.

- **Activo de Información:** Datos o información propiedad de la E.S.E. que se almacena en cualquier tipo de medio y que es considerada por la misma como sensible o crítica para el cumplimiento de los objetivos misionales.
- **Sistema de Información:** Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.
- **Propietario de Activos de Información**: En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.
- **Tecnología de la Información**: Conjunto de hardware y software operados por la entidad o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.
- **Evaluación de Riesgos:** Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto.
- **Administración de Riesgos:** Proceso de identificación, control y reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Responsable de Seguridad Informática:** Coordinador de Sistema, su función principal es supervisar el cumplimiento de la presente Política.
- **Grupo responsable de Seguridad Informática:** Grupos de apoyo creado en dependencias de la E.S.E. que manejan información sensible o crítica y que se encargan de velar por el cumplimiento de esta política. Están conformados por funcionarios o contratistas de la dependencia que tengan formación en temas de seguridad de la información.
- **Incidente de Seguridad Informática:** Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.
  Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento amenaza de romper los mecanismos de seguridad existentes.
- **Cadena de custodia:** En el ámbito de la seguridad de la información La cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.

15. REFERENCIAS

- **ISO 27001.** Sistemas de gestión de Seguridad en la Información– Requerimientos.
- **ISO/IEC 13335-1:2004.** Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones.
- **ISO/IEC TR 13335-3:1998**. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI.
- **ISO/IEC 13335-4:2000.** Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas.
- **ISO 14001:2004.** Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso
- **ISO/IEC TR 18044:2004**. Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información.
- **ISO/IEC 19011:2002.** Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental
- **ISO/IEC Guía 62:1996.** Requerimientos generales para los organismos que operan la evaluación y certificación/registro de sistemas de calidad.
- **ISO/IEC Guía 73:2002.** Gestión de riesgo –Vocabulario – Lineamientos para el uso en estándares.
- **NIST SP 800-30.** Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información.
- **ISO 9001:2000.** Sistemas de gestión de calidad – Requerimientos.

Actualizó	Revisó	Aprobó
YENNY ALEXANDRA HERRERA ASESORA CALIDAD GUSTAVO ADOLFO GÓMEZ LÓPEZ INGENIERO DE SISTEMAS	GLORIA PATRICIA LONDOÑO SUBGERENTE ADMINISTRATIVA Y FINANCIERA	DANIEL ALCIDES VERGARA GERENTE GENERAL