HOSPITAL UNIVERSITARIO DE SINCELEJO E.S.E

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

¡Un Hospital De Brazos Abiertos!

HOSPITAL UNIVERSITARIO DE SINCELEJO E.S.E

PROCESO: GESTIÓN ADMINISTRATIVA

SUBPROCESO: GESTIÓN DE LAS TICS

DOCUMENTO: PLAN

CÓDIGO: AGATIPL4

VERSIÓN No: 1

Aprobó: 22/01/2024
Nombre: Ruby Burgos Iglesias
Cargo: Gerente
Revisó: 18/01/2024
Nombre: Arnaldo Sánchez
Cargo: Subgerente Administrativo
Elaboró: 18/01/2024
Nombre: Oriana Corrales Peñates
Cargo: Gestor TICS

Tabla de Contenido

1. INTRODUCCIÓN 5
2. OBJETIVO 5
   2.1. Objetivo General 5
   2.2. Objetivos específicos 5
3. ÁMBITO DE APLICACIÓN 6
4. DEFINICIONES 6
5. RESPONSABLES 6
6. CAPITULOS 8
   6.1. MARCO NORMATIVO ..... ¡Error! Marcador no definido.
   6.2. Análisis de la situación Actual ..... ¡Error! Marcador no definido.
   6.2.1. Sede Sincelejo ..... ¡Error! Marcador no definido.
   6.2.2. Sede Corozal ..... ¡Error! Marcador no definido.
   6.2.3. Sede Betulia ..... ¡Error! Marcador no definido.
   6.2.4. Sede San Marcos. ..... ¡Error! Marcador no definido.
7. ESTRATEGIAS DE LA SEGURIDAD DE LA INFORMACION 12
8. CONTROL DE PORTAFOLIO DE PROYECTOS / ACTIVIDADES ..... ¡Error! Marcador no definido.
9. CONTROL DE CRONOGRAMA DE ACTIVIDADES ..... ¡Error! Marcador no definido.
10. RIESGOS Y CONTROLES 27
11. CONTROL DE CAMBIOS 28

1. INTRODUCCIÓN

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

2. OBJETIVO

2.1.Objetivo General

Minimizar y controlar los riesgos asociados con los sistemas de información y la infraestructura tecnológica que intervienen en el manejo y custodia de la información en el Hospital universitario de Sincelejo E.S.E y sus sedes San marcos, Corozal y Betulia.

2.2. Objetivos específicos

- Concientizar y comprometer a todos los funcionarios del Hospital y sus sedes sobre la necesidad e importancia de gestionar de manera adecuada los sistemas de información y los recursos tecnológicos, mitigando los riesgos inherentes a los que esto conlleva.
- Promover la cultura de la administración de riesgos en la seguridad y privacidad de la información creando conciencia al interior del Hospital de los beneficios que trae su aplicación y los efectos para la entidad por su desconocimiento y una posible ejecución.

3. ÁMBITO DE APLICACIÓN

Este plan suministra metodologías y conceptos que ayudarán a la administración y gestión de los riesgos; orienta sobre las actividades y buenas prácticas aplicadas a los procedimientos que tienen que ver con el uso y custodia de la información, identificando los riesgos, su valoración y la definición de opciones de manejo que pueden requerir la posible formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

4. DEFINICIONES

Para la gestión del riesgo del Hospital Universitario de Sincelejo, se deben tener en cuenta los siguientes términos y definiciones:

Amenaza: es un escenario externo o interno que puede mediante una vulnerabilidad causar un daño o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una omisión o debilidad que puede estar presente en diferentes escenarios, en la tecnología, en las personas o en los procedimientos y las políticas.

Probabilidad: es la posibilidad de ocurrencia para que la amenaza utilice la vulnerabilidad para lograr materializar el riesgo.

Impacto: son las causas o consecuencias generadas por un riesgo una vez sea materializado.

Riesgo: suceso que tendrá una consecuencia negativa sobre los procesos, esto es, en un escenario cuando una amenaza puede aprovechar una vulnerabilidad para generar un impacto negativo al core del negocio evitando cumplir sus objetivos.

Riesgo inherente: es aquel que tiene una entidad o proceso, en la no presencia de controles y/o acciones para modificar su probabilidad de ocurrencia y su impacto causado.

Riesgo residual: Es el riesgo que aún sigue luego de establecer y aplicar los controles para administrarlos.

Administración de riesgos: es una serie de etapas ordenadas de manera secuencial y que se deben ejecutar para el adecuado manejo de los riesgos.

Valoración del riesgo: se genera la identificación y evaluación de los controles con el fin de prevenir la ocurrencia del riesgo o reducir los efectos conforme su materialización. En el período

de valoración del riesgo se establece el riesgo residual, la ruta de gestión a seguir, y si es requerido o no.

Back up: Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información o ficheros en varios disquetes y que además la comprime.

Correo electrónico: Mensajes, documentos, archivos que se envían personas a través de Internet o de una red.

CPU (Unidad Central de Proceso): Carcasa donde van montados los principales componentes del ordenador. Puede ser de sobremesa, todo en uno, minitorre, semitorre y torre.

Cookies: Mecanismos que permiten a los gestores de cada página web grabar las entradas y salidas de los usuarios que acceden a su servidor.

Dirección IP: cifra numérica, ordenada y separadas por punto que identifica a un dispositivo en una red IP.

Escritorio: Pantalla inicial o espacio de trabajo que aparece al cargar el sistema operativo, sobre el cual vamos a realizar todo nuestro trabajo.

Explorador (Navegador): Aplicación mediante la cual podemos visualizar páginas Web de Internet (en inglés browser). Los más utilizados son Internet Explorer y Chrome.

Firewall: Dispositivos de seguridad que filtra las entradas no autorizadas.

Gigabyte (GB): Medida de 1.000 Mb (unos 1.000 millones de caracteres).

Internet: Red de redes mundial. Telaraña o entramado mundial. También llamada World Wide Web (WWW), conjunto de redes que permiten la comunicación de millones de usuarios de todo el mundo.

Informática: La informática o computación es la ciencia que estudia los métodos y técnicas para almacenar, procesar y transmitir información de manera automatizada, y más específicamente, en formato digital empleando sistemas computarizados

Password: Clave secreta personal para acceso.

Red de Área Local (LAN): Grupo de equipos conectados en un mismo lugar.

Sitio Web: Grupo de páginas Web relacionadas entre sí.

Software: Parte lógicas o blandas de un ordenador.

Sistema: Conjunto formado por el hardware y software que componen la parte esencial del ordenador.

Web: World Wide Web, Internet. Zona gráfica compuesta por millones de páginas Web y a la cual accedemos por medio de un navegador.

Mantenimiento: Conjunto de operaciones y cuidados necesarios para que instalaciones, edificios, industrias, etcétera, puedan seguir funcionando adecuadamente.

5. RESPONSABLES

Para lograr los objetivos de la administración del riesgo en la seguridad y privacidad de la información se depende no solo del plan, también de las partes involucradas y su participación activa, es preciso identificar los actores que intervienen.

Directivos: Aprueban los lineamientos conceptuales y metodológicos definidos en el mapa de riesgos institucionales con respecto a la seguridad y privacidad de la información de la entidad, es responsable de fortalecer e incentivar las políticas allí definidas dando cumplimiento a la administración del riesgo.

Integrantes de los procesos tanto misionales como administrativos: Identifican, analizan, evalúan y valoran los riesgos del proceso o subproceso por lo menos una vez al año, si bien están apoyados por el profesional en calidad y el profesional en sistemas, son los responsables de garantizar que en el proceso se definan los riesgos de la información que le competen, se establezcan los controles y se adelanten las actividades para mitigarlos.

Contratistas: Ejecutar en sus funciones, los controles y acciones definidas en los lineamientos de la administración del riesgo, también pueden aportar a la identificación de posibles riesgos que puedan afectar la información institucional.

Control Interno: Es su responsabilidad verificar y evaluar la elaboración, la visibilización, el seguimiento y el control del mapa de riesgos, conforme a la guía de administración de riesgo.

6. CAPITULOS

6.1. Gestión del Riesgo

El riesgo se define como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y pueda ocasionar un potencial daño a la organización”.

El Hospital Universitario de Sincelejo E.S.E., sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

TIPOS DE RIESGOS

Riesgo Estratégico: Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

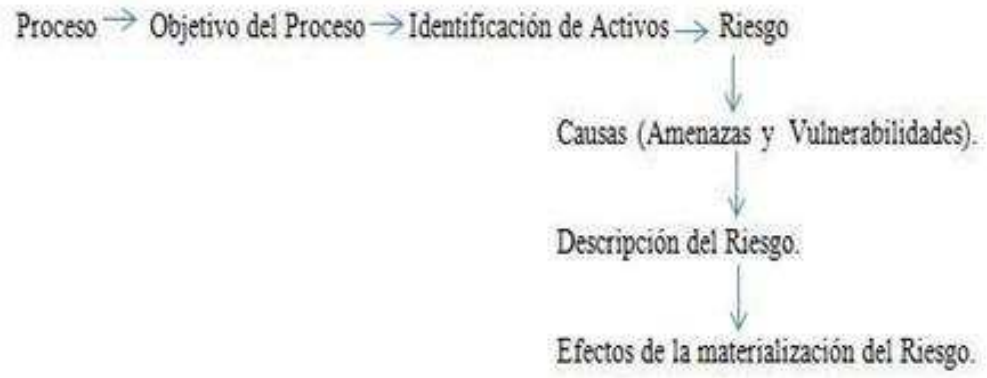
Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

6.2. Referencia propósito del plan de gestión de riesgo de la seguridad de la información

Preparación de un plan de respuesta a incidentes que soporte la seguridad de la información al interior de la entidad.

6.2.1.1. Identificación del riesgo



6.2.1.2. Descripción de vulnerabilidades

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, se encontraron otras amenazas e impactos como los siguientes:

Servidores y centro de cómputo.

El centro de cómputo Hospital universitario de Sincelejo E.S.E y sus sedes San marcos, Corozal y Betulia requiere de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada e ininterrumpida, sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, piso falso entre otros).

No se cuenta con contratos de mantenimiento vigente y apropiado con empresas y personal técnico calificado y debidamente autorizado.

Estaciones de trabajo.

Préstamo de usuarios y contraseñas de los usuarios de equipos de cómputo para el ingreso a sistemas operativos, así como para el ingreso a los diferentes aplicativos de la institución.

No existen UPS suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

Provocación por descuido o desatención emergencias como desconexión de la de la red; daño de los equipos, etc.

La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.

Del mantenimiento de las estaciones de trabajo.

No se cuenta con contratos de mantenimiento vigente y apropiado con empresas y personal técnico calificado y debidamente autorizado.

Red de Datos.

No hay adecuado suministro de fluido eléctrico continuo para equipos de misión crítica, se requiere de UPS que permitan mantener y garantizar la continuidad de los servicios de fluido eléctrico durante las caldas de voltaje.

Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad. No existe una estructura o protocolo fijo y establecido para la infraestructura física de la entidad.

Acceso físico a instalaciones.

Los accesos no son debidamente registrados, controlados y monitoreados, para identificar el mal uso potencial de los sistemas de información y así mitigar el riesgo de pérdida de información.

Permiten el acceso de terceros a información institucional, datos confidenciales o sensibles de los proyectos que son de propiedad o que son administrados por el Hospital Universitario de Sincelejo E.S.E.

Sistema Operativo y herramientas ofimáticas.

Algunos de los sistemas operativos (Windows) y herramientas ofimáticas (Office) ya cumplieron su ciclo de vida y por tanto Microsoft no brinda soporte técnico. Sin el soporte de Microsoft, ya no se reciben actualizaciones de seguridad que pueden ayudar a proteger el equipo de virus, spyware y otros softwares malintencionados, que pueden robar o dañar la información.

Copias de seguridad.

Existen procesos de copias de seguridad establecidos. Se realizan diariamente copias de seguridad de los datos manejados por el sistema de Información, pero los usuarios no se han concientizado de realizar las copias de su información relevante. No se ha podido automatizar debido a la falta de recursos que lo permitan y existe riesgo de pérdida de información.

Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

Otros.

Dejar elementos que puedan disminuir la vida útil del equipo (teclados, Mouse e impresoras), elementos tales como tintas, bebidas o alimentos.

Utilizar las oficinas y equipos como objeto de tertulia o juegos.

7. ESTRATEGIAS DE LA SEGURIDAD DE LA INFORMACION

Infraestructura física

Las políticas de seguridad en cuanto a la infraestructura física, involucran servidores, estaciones de trabajo, periféricos y otros equipos soporte de los programas de computador y de la operación de la institución. Los recursos tecnológicos son de uso exclusivo para asuntos relacionados con las actividades del Hospital Universitario de Sincelejo E.S.E y sus sedes San marcos, Corozal y Betulia; por tal motivo, todos los usuarios deben guiarse por las políticas de uso y seguridad de la información, así como por las normas y procedimientos que para tal fin sean emitidos por la Gerencia a través de la Oficina de Planeación

Servidores y centro de cómputo

Cuando existan equipos de cómputo de la Institución que sean de propósito específico y tengan una misión crítica asignada, la Subgerencia Administrativa y Financiera, la Oficina de Planeación, y Sistemas, deberán garantizar que estén ubicados en un área que cumpla con los requerimientos de seguridad física, control de acceso, condiciones ambientales y alimentación eléctrica necesaria.

Toda nueva adquisición y la implantación de hardware o componentes, se deben cumplir con los estándares técnicos y de compatibilidad definidos por el área de Sistemas del Hospital Universitario de Sincelejo E.S.E. y la Subgerencia Administrativa y Financiera según los avances tecnológicos vigentes.

La implementación de modificaciones, adiciones o de nuevo hardware debe contemplar la revisión de las políticas de seguridad, de forma que se realicen los ajustes a las ya existentes y/o incorporación de nuevas políticas a que haya lugar.

Cuando existan servicios de procesamiento de información prestados por terceros o compañías externas al Hospital Universitario de Sincelejo E.S.E, se deben exigir adecuados y oportunos niveles de servicio que se ajusten a los estándares de calidad, necesidad y seguridad de la información requeridos por la entidad.

Todos los equipos de cómputo y componentes deben estar completa y exhaustivamente probados y aceptados de manera formal por parte del área de Sistemas, antes de ser puestos en producción.

Todos los equipos de propiedad del Hospital Universitario de Sincelejo E.S.E deben contar con contratos de mantenimiento vigente y apropiado con empresas y personal técnico calificado y debidamente autorizado.

Todo proveedor que administre instalaciones externas al Hospital Universitario de Sincelejo E.S.E. y sus sedes San marcos, Corozal y Betulia debe conocer y aplicar las políticas de seguridad y de confidencialidad de la información establecidas por el Hospital Universitario de Sincelejo E.S.E. Por lo anterior, en las obligaciones contractuales estará explicito el cumplimiento a las políticas de la institución y las condiciones sancionatorias en caso de incumplimiento.

La Subgerencia Administrativa del Hospital Universitario de Sincelejo E.S.E es la única autorizada para dar de baja los equipos del centro de cómputo de propiedad de la institución, de acuerdo con los criterios técnicos establecidos dados por el personal autorizado del área de Sistemas, garantizándose que se han eliminado los riesgos de confidencialidad y seguridad de la información.

Todas las fallas de hardware de los sistemas de información deben ser reportadas oportunamente y ser atendido por personal del área de Sistemas.

Estaciones de trabajo

La oficina de almacén deberá contar con un inventario de todos los equipos de cómputo del Hospital Universitario de Sincelejo E.S.E. y sus sedes San marcos, Corozal y Betulia, estableciendo la condición de adquisición de cada uno de ellos (Propiedad, comodato, arriendo, convenio, etc.).

Se permite que los usuarios utilicen estos recursos (estaciones de trabajo) para facilitarles el desempeño de sus labores. El uso adecuado de este recurso es una obligación del usuario, por tanto, puede ser revocado en cualquier momento, cuando se demuestre un mal uso de este.

Solamente los funcionarios del área de sistemas podrán acceder y manipular los equipos adquiridos a cualquier título por el Hospital Universitario de Sincelejo E.S.E. y entregados como herramienta de trabajo a los funcionarios o contratistas, quedando por ende prohibida cualquier manipulación, alteración, mantenimiento o en si cualquier afectación a los equipos de los servicios de la institución, así mismo la instalación o desactivación de los mismos.

Los directorios de datos y las estructuras deben ser establecidos por el propietario de la información, así como las restricciones de acceso a tales directorios y aplicar según la necesidad.

El Hospital Universitario de Sincelejo E.S.E, apoyándose en la oficina de planeación y el área de sistemas debe seleccionar, adquirir, instalar y mantener los softwares antivirus apropiados para la salvaguardar la información, en todas y cada una de las estaciones de trabajo o equipos portátiles de la entidad y cada una de sus sedes.

Se debe reportar todas las novedades para el manejo de los incidentes causados por virus, la cual, requerirá el análisis, seguimiento y resolución por parte del área de sistemas.

Está expresamente prohibido a los usuarios de equipos de cómputo que posean contraseñas para el ingreso a sistemas operativos, así como para el ingreso a los diferentes aplicativos de la institución, PRESTAR SUS USUARIOS Y CONTRASEÑAS. De requerirse creación de nuevos usuarios, debe hacerse una solicitud por parte del jefe de área dirigida a la oficina sistemas con una antelación de 24 Horas a través del correo electrónico depende de la sede:

Sede principal Sincelejo: sistemas@husincelejo.com.co
Sede Corozal: sistemas@esehospitalcorozal.com
Sede Betulia: sistemas.esebetulia@gmail.com

Sede San marcos: sistemas@esehospitalregionalsanmarcos.gov.co
Está expresamente prohibido el uso de recursos de cómputo para fines personales, excepto cuando se adquiere el permiso especial autorizado por el coordinador del área o jefe inmediato y solo por el tiempo autorizado.

Los usuarios no podrán provocar por descuido o desatención emergencias como parada de las máquinas servidoras ante un posible error grave del sistema; desconexión de las mismas de la red; caldas de la red; incendio, etc.

Los usuarios deberán tener el debido cuidado para evitar averiar o deteriorar de forma alguna el material hardware (equipo de cómputo e impresoras).

Los usuarios no podrán modificar la configuración estándar preestablecida (hardware o software) de los ordenadores de las oficinas (alteración de direcciones ethernet o I.P., cambio del nombre, cambio de dominio, alteración en el arranque del ordenador).

Todo equipo de cómputo (Monitor – CPU) debe estar conectado a la canaleta de corriente regulada claramente identificada. No se deben conectar a las canaletas de corriente regulada impresoras u otros elementos diferentes a CPU y monitores, como, por ejemplo: radios, máquinas de aseo, elementos para verificar billetes o equipos médicos. En caso en que la oficina no cuente con la acometida correspondiente deberá existir por lo menos un multitoma que sirva de puente entre la entrada de corriente alterna externa y la alimentación del equipo, para moderar los picos de voltaje.
Todas las fallas de hardware de los sistemas de información deben ser reportadas oportunamente y ser atendido por personal del Área de Sistemas.

Del mantenimiento de las estaciones de trabajo

Al área de sistemas de información, corresponde EXCLUSIVAMENTE la coordinación del mantenimiento preventivo y correctivo de los equipos de cómputo pertenecientes al Hospital Universitario de Sincelejo E.S.E.

La Oficina de Planeación a través del área de Sistemas mantendrá registro de cada mantenimiento preventivo y correctivo de los equipos de cómputo pertenecientes a la institución

De la reubicación y/o reasignación del equipo de cómputo

Nunca se podrá permitir la reubicación o retiro de elementos o del equipo de cómputo/Impresora sin la presencia de funcionarios de Almacén y sistemas y sin la autorización del Jefe de Oficina, Subgerente o de quien figure como responsable del mismo.

Del encendido del equipo de cómputo

Todo equipo de cómputo se debe encender tal como se muestra en la siguiente gráfica:

Del apagado del equipo de cómputo.

Una vez finalizada su jornada de trabajo, cada usuario deberá dejar el equipo en correcto estado, realizando el debido apagado por medida de seguridad y para preservar la vida útil del equipo. Antes de apagar un equipo se deben tener en cuenta las siguientes consideraciones:

Vaciar carpetas temporales.
Depurar los espacios compartidos que han sido utilizados: Las carpetas compartidas creadas en cada máquina poseen una finalidad temporal, por este motivo una vez utilizada la misma, debe borrarse la información almacenada en ella.
Eliminar Cookies.
Cerrar cada aplicación ejecutada en el computador. Una vez terminada la jornada laboral, se deben cerrar los aplicativos que se utilizaron durante la misma. Cada software trae su correspondiente forma de cierre y debe efectuarse en la forma que este lo indique.
Extraer todo medio externo de las unidades, como cd, memorias USB u otros. Esto se realiza con el fin de evitar inconvenientes al momento de arrancar nuevamente los equipos de cómputo.
No dejar claves personales expuestas al uso público. No entregar, revelar o exponer las claves al uso público. Esto permitirla que un usuario diferente al propietario de la misma realizara consultas, transacciones o eliminación de información.
Cerrar la sesión de red respectiva. Una vez terminada la jornada laboral, cada usuario debe garantizar que termina y cierra su sesión de trabajo en el computador en el que se encontraba

desempeñándose. No se deben iniciar sesiones en equipos de cómputo cuyo usuario anterior no haya terminado la misma (usuarios de sistema operativo y usuarios de aplicativos de la institución), así como recordar que MAXIMO SE PUEDEN ABRIR DOS (2) SESIONES de trabajo en los sistemas de información de la entidad. El abrir más de las mencionadas genera lentitud en cada estación y por consiguiente demora en procesos.

Todo equipo de cómputo se debe apagar tal como se muestra en la siguiente gráfica:

Periféricos

La información clasificada como altamente confidencial nunca puede enviarse a una impresora en red sin que haya una persona autorizada para salvaguardar su confidencialidad durante y después de la impresión.

Todos los equipos periféricos de propiedad del Hospital Universitario de Sincelejo E.S.E deben contar con los servicios de mantenimiento apropiado, realizado por personal técnico calificado y debidamente autorizado.

Todas las fallas de hardware de los sistemas de información deben ser reportadas oportunamente y ser atendido por personal del área de sistemas.

Red de datos

Red física

La Oficina de Planeación, a través del área de sistemas debe instalar y/o mantener, con personal calificado y debidamente autorizado, la red de datos y voz, con el fin de garantizar la operación, seguridad e integridad.

Cualquier equipo y/o elemento activo y/o pasivo de la red que no se utilice debe ser desactivado y controlado.

No está permitido hacer seguimiento o monitoreo de puertos o tráfico de red, por parte de personas diferentes a las autorizadas por el área de sistemas.

La red de datos y voz debe estar diseñada y configurada para contar con un alto rendimiento, confiabilidad y seguridad, ajustándose a las necesidades del Hospital Universitario de Sincelejo E.S.E y al mismo tiempo, contar con un alto grado de control de acceso, que permita el correcto seguimiento y control de los usuarios.

La instalación, desinstalación y manejo de los Access Point y equipos de transmisión de datos es competencia exclusiva del área de sistemas.

La administración de la red del Hospital Universitario de Sincelejo E.S.E debe ser realizada por personal debidamente calificado. Los administradores, los propietarios del activo y los usuarios deben preservar su integridad, seguridad y desempeño.

El acceso remoto a la red del Hospital Universitario de Sincelejo E.S.E y a sus recursos, solamente se facilitará a los usuarios autorizados por la Gerencia de la institución y el control de dicho acceso se realizará a través del área de sistemas.

Los equipos de misión crítica, requieren de UPS que permitan mantener y garantizar la continuidad de los servicios de fluido eléctrico durante las caídas de voltaje

Red Inalámbrica.

El área de sistemas debe garantizar que personas no autorizadas a la red WIRELESS- Hospital Universitario de Sincelejo E.S.E. accedan a los datos de la entidad.

Los jefes de área, funcionarios, contratistas y visitantes no podrán instalar Access Point (AP) de propiedad de los mismos, sin la expresa autorización del área de sistemas de Información. En el caso de encontrarse equipos AP instalados, el área de sistemas de información los desinstalará para proteger la red de la entidad.

Red de Voz.

Red Telefónica.

Toda nueva adquisición, pruebas, instalación e implementación de elementos o soluciones de telefonía en general deben cumplir con los estándares técnicos y compatibilidad definidos por el funcionario o área encargada de la administración de la telefonía en conjunto con el área de sistemas.
Todos los sistemas de marcación rápida deben incluir características de seguridad que protejan la información confidencial y sensible.
Para el personal que da instrucciones vía telefónica o que brinde información, se debe verificar la identidad de la persona que recibe la información y si tiene permiso para recibir esta información.
En ningún caso podrá grabarse información confidencial o sensible en máquinas de audio respuesta y/o sistemas de correos de voz.
No permitir el uso de los equipos de telefonía fija por personal ajeno a la entidad.

Telefonía Móvil.

No está permitido transmitir información confidencial.
Los teléfonos celulares deben tener activados los controles de acceso o contraseñas y en su directorio interno no debe guiar a las personas ajenas al celular a qué tipo de funcionario se está refiriendo, es decir, la ocupación o cargo dentro del Hospital Universitario de Sincelejo E.S.E.
El teléfono celular no debe identificar a que área del Hospital Universitario de Sincelejo E.S.E pertenece.
Los teléfonos celulares de los directivos no deben mostrar la identificación del número celular del que se llama.
Es obligación de los usuarios en el momento de pérdida del celular bloquear la línea telefónica.
No permitir que personas o terceros lo utilicen para su uso personal.
Deben tener activados la localización, en caso de pérdida

Acceso físico a instalaciones

Los datos de la entidad deben ser administrados y configurados apropiadamente, para salvaguardarlos de ataques físicos, de accesos no autorizados por la red y/o delincuentes digitales.

El acceso debe ser registrado, controlado y monitoreado por el propietario del activo y/o en su

defecto por el depositario del mismo, para identificar el mal uso potencial de los sistemas de información y así mitigar el riesgo de pérdida de información.

Los controles de acceso para la información altamente sensible o sistemas de alto riesgo deben ajustarse de acuerdo con la clasificación de los activos que se deseen proteger.

Documentación del Hardware

La documentación es un requisito para todas las tecnologías de información y comunicaciones, procesos y procedimientos del macro proceso de sistemas de Información del Hospital Universitario de Sincelejo E.S.E. Dicha documentación debe mantenerse actualizada; igualmente garantizar su disponibilidad y confidencialidad.
Los documentos deben archivarse, de acuerdo con su estado de clasificación, en instalaciones seguras, con restricción de acceso a personal no autorizado, cumplir con las mínimas condiciones ambientales, eléctricas y de extinción de incendios, entre otros.
Debe mantenerse un inventario formal y actualizado del hardware de la entidad.

Operación y Administración de Sistemas

Las tecnologías de información del Hospital Universitario de Sincelejo E.S.E deben ser manejados por administrador(es) de sistemas debidamente calificado(s), quien(es) será(n) responsable(s) de supervisar el funcionamiento diario y de seguridad de las mismas.
Los administradores deben estar completamente capacitados y contar con la experiencia adecuada en la amplia variedad de hardware, software y procesos utilizados por el Hospital Universitario de Sincelejo E.S.E. Además, deben contar con los conocimientos y manejo de una gran variedad de riesgos relacionados con la seguridad de la información.
Únicamente personal calificado y autorizado por el proveedor (en el caso en que el elemento de la TICS se encuentre en garantía), o técnicos autorizados por el área de sistemas de información del Hospital Universitario de Sincelejo E.S.E. pueden reparar las fallas en hardware o software.
Los reportes de transacciones y/o procesamiento deben revisarse periódicamente por personal adecuadamente calificado y entrenado.
Los usuarios y/o responsables de los servidores de cómputo deben bloquear sus equipos, en caso de abandonar temporalmente su sitio de trabajo o salir del sistema ante una prolongada ausencia.

SOFTWARE

Control de acceso

El área de sistemas establece los estándares de control de acceso a la información. Permiten el acceso solamente a personal autorizado para realizar funciones propias del Hospital Universitario de Sincelejo E.S.E.
El acceso al sistema de información es autorizado por los jefes o coordinadores funcionales haciendo uso del procedimiento establecido para esto. Dicho acceso incluye los privilegios y roles suficientes para desempeñar las funciones de su cargo. El registro de estos permisos de acceso, son considerados documentos de alta confidencialidad, salvaguardados como tales y sujetos a control y auditoria.
La definición de roles, permisos y el control de acceso de los usuarios al sistema de información será determinado por el área responsable de generar y procesar los datos involucrados.
La cancelación del acceso al sistema de información a funcionarios del Hospital Universitario de Sincelejo E.S.E. y demás usuarios de los sistemas será responsabilidad de los jefes o coordinadores funcionales, con el fin de revocar los accesos, incluyéndose los privilegios y roles.
Las contraseñas son personales e intransferibles, no se pueden compartir con ninguna otra persona, bajo ninguna circunstancia. Tampoco se pueden generar contraseñas en blanco y debe exigirse actualizar la contraseña periódicamente. Los usuarios son responsables de tomar las debidas precauciones para mantener la confidencialidad de su contraseña para evitar el acceso de personal no autorizado a la información y/o a los recursos.
Solamente los funcionarios autorizados tienen acceso a los datos confidenciales o sensibles de los proyectos que sean de propiedad o que sean administrados por el Hospital Universitario de Sincelejo E.S.E. y sus funcionarios.
El acceso de terceros a información institucional únicamente es autorizado por el propietario del activo. Esto bajo las condiciones de seguridad, confidencialidad, disponibilidad, control y auditoria.
Se manejarán los certificados digitales cuando así se requiera, para la autenticación de las partes, integridad de la transacción, confidencialidad y/o no repudio, en la emisión y/o recepción de información electrónica.

Del Control de Acceso a los equipos de cómputo.

Todos y cada uno de los equipos son asignados a un usuario, por lo que es de su competencia y responsabilidad hacer buen uso de los mismos.
El área de sistemas tiene la facultad de acceder a cualquier equipo de cómputo con propósitos de soporte, sin que de esta manera se vea comprometida la confidencialidad y privacidad de la información manejada en el mismo, toda vez que solo se permite en las instalaciones del hospital

y en los equipos entregados como herramienta de trabajo para desarrollar actividades institucionales y nunca personales. Así como de aquellos equipos autorizados los ingresos y que se cuelguen a la red institucional.

Del Control de Acceso local a la red y acceso remoto.

El Área de sistemas asignará a cada usuario una cuenta personal de identificación en la red y una contraseña para que pueda utilizar el equipo; formar parte de la intranet del hospital y contar con todos los servicios de la red. Se debe tener en cuenta, que servicios como acceso remoto a equipos, uso de Internet, acceso a carpetas compartidas, acceso a impresoras de red, solo estarán disponibles si se ha realizado una correcta validación de entrada a la computadora.
En caso de tener inconvenientes con la validación del usuario deberá informar oportunamente al área de sistemas.
La cuenta personal creada para cada usuario se podrá utilizar en todo equipo de cómputo, pero los recursos de red solo estarán disponibles para las personas autorizadas. Llámese recursos de red a los archivos, carpetas, impresoras, unidades de CD e Internet.
Todo equipo de cómputo que esté conectado a la red del hospital, debe sujetarse a los procedimientos de acceso que emite el área de sistemas.

De la Instalación de Software.

Solamente la oficina sistemas podrá instalar programas en los computadores.
Está expresamente prohibido el uso de computadores con programas de cualquier tipo que no estén licenciados para uso institucional. Esta prohibición es extensible aún en el caso de tener que instalarse en soporte fijo o de manera permanente.
Todos los usuarios podrán usar los programas instalados en cada máquina. Para la instalación de nuevos programas, se realizará una petición formal a la oficina de sistemas

Mal Uso del Software.

Los Usuarios no podrán efectuar copias, instalaciones, modificaciones, adaptaciones o aplicar ingeniería de reverso en ningún software institucional.
Los usuarios deberán informar a su jefe inmediato cuando tengan conocimiento de cualquier hecho que tengan que ver con algún tipo de violación al uso adecuado y legal de software o de los derechos respectivos de autor.

Protección Jurídica de los programas del computador - Marco Legal

El área de sistemas , vigilará el cumplimiento de la normatividad legal vigente en materia de

protección jurídica sobre los programas del computador, por tanto queda absolutamente prohibido utilizar programas no licenciados o que no cumplan con la reglamentación y autorizaciones respectivas sobre derechos de autor ya que su inobservancia constituye un delito el cual en el evento de presentarse será reportado a la autoridad competente y el responsable de equipo de cómputo será el llamado a atender los requerimientos de los entes competentes.

Cuando se adquieran programas de computador de cualquier tipo, se exigirá la autorización del titular de derechos patrimoniales, para lo cual se exigirán siempre las licencias, mantenimientos, autonomía, condiciones, paquetes de software, etc., y se definirá quien es el titular de los derechos de autor, así como las condiciones bajo las cuales el hospital podrá modificar, disponer y en general hacer uso del programa de computador, estableciendo el grado de dependencia tecnológica que eventualmente pueda llegar a constituir un riesgo en la contratación estatal, lo cual será garantizado tanto en los términos de referencia, como en la recepción y la exigencia de garantías como mantenimientos o prevención de dependencia.

Desarrollos WEB.

El sitio web es un recurso de información, imagen y divulgación para el Hospital Universitario de Sincelejo E.S.E; contiene recursos de seguridad que la protegen de intrusos. Solamente los funcionarios calificados y autorizados desarrollan y actualizarán el sitio web debidamente documentado y probado.
Las actualizaciones del software deben ser probadas por personal debidamente calificado antes de ser implementados en un ambiente de producción. Todo el software aplicativo debe contar con el nivel apropiado de soporte técnico para evitar que las operaciones críticas del Hospital Universitario de Sincelejo E.S.E lleguen a comprometerse y garantizar que los problemas de software se manejen de manera eficiente con una solución disponible y en tiempo aceptable, de tal manera que no afecte la continuidad del servicio.
Los fallos del software deben ser registrados formalmente y reportados a los funcionarios responsables de soporte y mantenimiento de software, haciendo uso de los procedimientos establecidos para ello.
Es responsabilidad de los usuarios ingresar información confiable y veraz a los Sistemas de Información.
El uso de datos reales para probar nuevos sistemas o modificaciones al sistema actual únicamente se podrá realizar bajo autorización, siempre y cuando se apliquen las normas establecidas que garanticen la seguridad de los datos.
Se debe proporcionar la capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de todos los nuevos aplicativos y/o sistemas de información, antes de su puesta en marcha.
Todos los sistemas nuevos y mejorados deben estar completamente soportados por una

documentación suficientemente amplia y actualizada. Además, no deben ser puestos en ambiente de producción sin contar con la documentación disponible.

Software de Motor de Base de Datos.

La transferencia e intercambio de datos e información sensible o confidencial solamente puede hacerse a través de las redes o copiarse a otro medio de almacenamiento, siempre que la confidencialidad e integridad de los datos se garantice mediante el uso de técnicas de encriptación. Donde se considere apropiado, la información y los datos sensibles o confidenciales siempre deben transmitirse en forma encriptado. Antes de la transmisión, siempre se deben considerar los procedimientos que se deben utilizar entre el remitente y el destinatario, y cualquier aspecto legal de la utilización de las técnicas de encriptación.
El almacenamiento de datos diario debe garantizar que los datos reales estén siempre disponibles para los usuarios autorizados y que las copias de seguridad sean tanto creadas como accesibles en caso de necesitarse.
La información creada y almacenada por los sistemas de información del Hospital Universitario de Sincelejo E.S.E debe retenerse por un período mínimo que se ajuste a los requerimientos legales.
Las bases de datos deben estar probadas completamente previamente a su puesta en producción tanto en la parte lógica como en su procesamiento
El respaldo de los archivos de datos del Hospital Universitario de Sincelejo E.S.E y la capacidad de recuperar tales datos es una prioridad crítica. El área de sistemas del Hospital Universitario de Sincelejo E.S.E es responsable de generar las directrices para garantizar que la frecuencia de realización de los procedimientos de copias de respaldo y los procedimientos de recuperación se ajusten a las necesidades de la entidad.
El área de sistemas de Información debe garantizar que se implementen las medidas para salvaguardar y proteger la integridad de los archivos de datos durante la recuperación y restauración; especialmente donde éstos puedan reemplazar archivos más recientes.
Solamente se podrán aplicar parches para corregir problemas del software donde se demuestre que es necesario y con la autorización del área de sistemas del Hospital Universitario de Sincelejo E.S.E. Estos deben provenir de una fuente reconocida y ser completamente probados antes de su implementación.
El proceso de copias de respaldo debe contemplar la validación del mismo, para garantizar su posterior utilización.
Toda falla de software debe ser reportada oportunamente y ser atendido por personal del área de sistemas.

Software de Sistema Operativo

La escogencia de contraseñas, su uso y manejo como medio de primera instancia del control de acceso a los sistemas, debe ajustarse a los lineamientos de políticas de seguridad, administración de plataformas informáticas y mejores prácticas. Particularmente, las contraseñas no se pueden compartir con ninguna otra persona, bajo ninguna circunstancia.
Solamente se podrán aplicar actualizaciones para corregir problemas del software donde se demuestre que es necesario y con la autorización del área de sistemas del Hospital Universitario de Sincelejo E.S.E. Estos deben provenir de una fuente reconocida y deben ser completamente probados antes de su implementación.
Las actualizaciones necesarias al sistema operativo de cualquier sistema computacional del Hospital Universitario de Sincelejo E.S.E deben contar con una plena identificación de los riesgos asociados y deben ser planeados cuidadosamente, así como también deben incorporar procedimientos de retroceso. Todas las actualizaciones deben ser consideradas como un proyecto formal.
Los sistemas operativos se deben monitorear periódicamente; estos se deben ajustar a todos los procedimientos asociados.
Los fallos del sistema operativo deben ser registrados formalmente y reportados a los funcionarios responsables de soporte y mantenimiento de software, haciéndose uso de los procedimientos establecidos para ello.
Toda falla del sistema operativo debe ser reportados oportunamente y atendido por personal del área de sistemas de Información.

Documentación.

Todos los aplicativos deben contar con la documentación necesaria para auto capacitación y/o consulta de la forma de operación, en el caso de usuario final y de la información técnica, en el caso de los funcionarios del área de sistemas del Hospital Universitario de Sincelejo E.S.E.
La documentación de uso del sistema debe responder a un estándar de elaboración de documentos de este tipo, de manera que sea universal en su forma, para entendimiento de los usuarios.
La documentación de uso del sistema estará disponible para los funcionarios del Hospital Universitario de Sincelejo E.S.E para su consulta en cualquier momento.
La documentación técnica será de uso restringido al personal autorizado por el área de sistemas del Hospital Universitario de Sincelejo E.S.E.

UTILIZACION DE LOS RECURSOS.

De la utilización de los recursos de la red.

Los usuarios de los equipos de cómputo por política de seguridad tienen asignadas cuentas de acceso a los sistemas para poder desarrollar sus labores, siendo dichas cuentas personales e intransferibles, lo que significa que por ningún motivo se deben prestar o revelar contraseñas.
Las contraseñas individuales no deben ser impresas, almacenadas en los sistemas o suministrada a cualquier otra persona. Queda prohibido y por medida de seguridad que los usuarios accedan al sistema utilizando la cuenta o contraseña de otro usuario.
Teniendo en cuenta que toda transacción queda registrada mediante este mecanismo, será responsabilidad personal los trámites y registros que se realice con cada cuenta de usuario. Por tanto, en el evento de no utilización o carencia de seguridad existe la posibilidad de cambiarla o deshabilitar, para lo cual el usuario informará oportunamente al área de sistemas, toda vez que solamente hasta que se informe a esta oficina se mantiene la responsabilidad personal de la cuenta.
Es responsabilidad directa del coordinador del área o jefe inmediato, informar de manera escrita al área de sistemas la creación de usuarios de red y de usuarios para los Sistemas de Información.

Del Manejo de Archivos.

Todo usuario debe guardar el máximo respeto al trabajo de los demás, no destruyendo o copiando archivos de otros usuarios, (salvo su autorización directa) o interrumpiendo sus sesiones por cualquier procedimiento.
Ante cualquier duda sobre el uso de los recursos de cómputo de las oficinas, consúltese en primera instancia las ayudas on-line o los manuales respectivos. En último extremo, acuda al personal del área de sistemas a través de una solicitud de soporte.
Se debe garantizar por cada usuario que las copias que se realicen de trabajos de la entidad puestos en carpetas compartidas o en intranet sean exclusivos para el manejo de información y trámites de la entidad, y bajo ningún aspecto se pueden difundir, manipular, editar o presentar para trámites ajenos a la entidad.

Recomendaciones en el uso de los equipos de cómputo.

No dejar elementos que puedan disminuir la vida útil del equipo (teclados, Mouse e impresoras), elementos tales como tintas, bebidas o alimentos.
Beber, comer o fumar mientras se trabaja en los equipos de cómputo.
Utilizar las oficinas y equipos como objeto de tertulia o juegos.

Realizar modificaciones a la configuración de los equipos de cómputo como: cambio del papel tapiz, cambio en los punteros del mouse o de protectores de pantalla, toda vez que estos corresponden a la imagen institucional entendida como corporativa y por ende obligatoria.
Realizar manipulaciones a los equipos de cómputo, impresoras, etc. Cuando se haga bloqueo de la pantalla, éste no ha de exceder la hora y media, en su defecto se deberá apagar la máquina posibilitando a otro usuario autorizado el uso de dicho equipo.

Carpetas compartidas.

Cada equipo de cómputo tiene un espacio (carpeta compartida) en disco duro, para colocar los documentos que ameriten ser compartidos y su permanencia allí será responsabilidad de cada usuario, dado que este espacio es de dominio exclusivo del personal de la entidad, el acceso al mismo es público, lo cual no exonera la debida reserva y responsabilidad en el manejo de esta información, de tal manera que por hacerse pública dentro de la institución, no por ello implica que deba ser de manejo público general.
El área de sistemas, no se responsabiliza por el uso de los datos en zonas compartidas, ni temporales, por tanto la información de cada área es responsabilidad de los funcionarios de la misma, quienes harán las copias de seguridad que consideren necesarias.
Toda información que requiera ser custodiada mediante copia de seguridad, deberá ser almacenada en la correspondiente carpeta creada en cada equipo de cómputo para este fin. De forma automática y mediante programación por parte del área de sistemas, se copiará la información puesta por el usuario en la carpeta antes mencionada. La información no se encuentre en la misma no se le efectuará proceso de copia de seguridad.

8. RIESGOS Y CONTROLES

A continuación se realiza una descripción de riesgos a los que se expone la entidad al no implementar un Plan de Tratamiento de Riesgo de Seguridad de la Información.

Riesgos	Controles
Daños físicos de los equipos tecnológicos	Mantenimiento preventivos y correctivos
Espionaje remoto	Software de seguridad perimetral
Mal funcionamiento del Software	Soporte de Software
Hurto de información	Cambios de contraseña – controles de acceso físico.
Falta de continuidad de los procesos asistencias y administrativos.	Existencia, implementación, desarrollo y evaluación de un Plan de Tratamiento de Riesgo de Seguridad de la Información

9. CONTROL DE CAMBIOS

Fecha del Cambio	Versión	Descripción del Cambio	Responsable
17/01/2024	1	Creación documento bajo un sistema integrado de gestión de calidad	Oriana Corrales Peñates – Gestor TICS