PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

JORGE ALBERTO
LEMUS BELLO
GERENTE

GUAMAL – MAGDALENA
2024

INTRODUCCIÓN

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.

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.

OBJETIVOS

OBJETIVO GENERAL

Definir actividades, que permitan planificar, desarrollar, monitorear y aplicar la de Gestión de Seguridad de la Información – de la E.S.E., para garantizar la seguridad y privacidad de la información.

OBJETIVOS ESPECÍFICOS

- Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.

- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.

- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

ALCANCE

Aplica a la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones generen, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

Así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación.

MARCO LEGAL

- **Ley 1273 de 5 de enero 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 23 de 1982:** Sobre derechos de autor

- **Ley Estatutaria 1266 de 2008:** Por la cual se dictan las disposiciones generales de 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. Para conocer más de esta Ley, Ley 1581 de 2012, la cual establece disposiciones generales para la Protección de Datos Personales.

DEFINICIONES

- **Riesgo**: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **Amenaza**: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Vulnerabilidad**: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **Probabilidad**: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

- **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Contratistas:** Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

- **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Guía**: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad

- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros

- **Procedimiento**: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

- **Rol**: Papel, función que alguien o algo desempeña.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

DIRECCIONAMIENTO ESTRATEGICO DE LA E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL, MAGDALENA

MISIÓN

Somos un hospital público de baja complejidad que ofrece servicios de salud con criterios de calidad, seguridad y oportunidad; contamos con un recurso humano idóneo comprometido con la mejora continua de los procesos asistenciales orientados hacia la satisfacción del usuario y su familia.

VISIÓN

En el 2023 seremos reconocidos como un hospital que ofrece servicios de salud oportunos y de calidad, apoyado en su equipo humano e infraestructura física y tecnológica, fijando como propósito el fortalecimiento de los servicios habilitados y dando apertura a nuevas estrategias de atención que permitan convertirnos en una institución eficiente y humanizada.

CÓDIGO DE INTEGRIDAD

El Código de Integridad es el principal instrumento de la Política de Integridad del MIPG, parte de la Dimensión de Talento Humano. El Decreto 1499 de 2017, en concordancia con el artículo 133 de la Ley 1753 de 2015 hizo extensiva su implementación diferencial a las entidades territoriales.

OBJETIVO DEL CÓDIGO DE INTEGRIDAD

Fomentar en los usuarios y funcionarios de la E.S.E la implementación de acciones de integridad que fortalezcan la cultura y clima organizacional, bajo acciones de servicio al usuario y su familia con eficacia y calidad humana

ALCANCE DEL CÓDIGO DE INTEGRIDAD

Los valores y lineamientos del presente Código serán asumidos y cumplidos de manera consciente y responsable por todos los servidores públicos y funcionarios vinculados a la E.S.E HOSPITAL NUESTRA SEÑORA DEL CARMEN y serán fomentados de manera especial por la Alta Dirección de la entidad, Equipo de Integridad y aliados claves como los comités en actividades de Talento Humano, interventores, líderes y coordinadores y jefes de áreas.

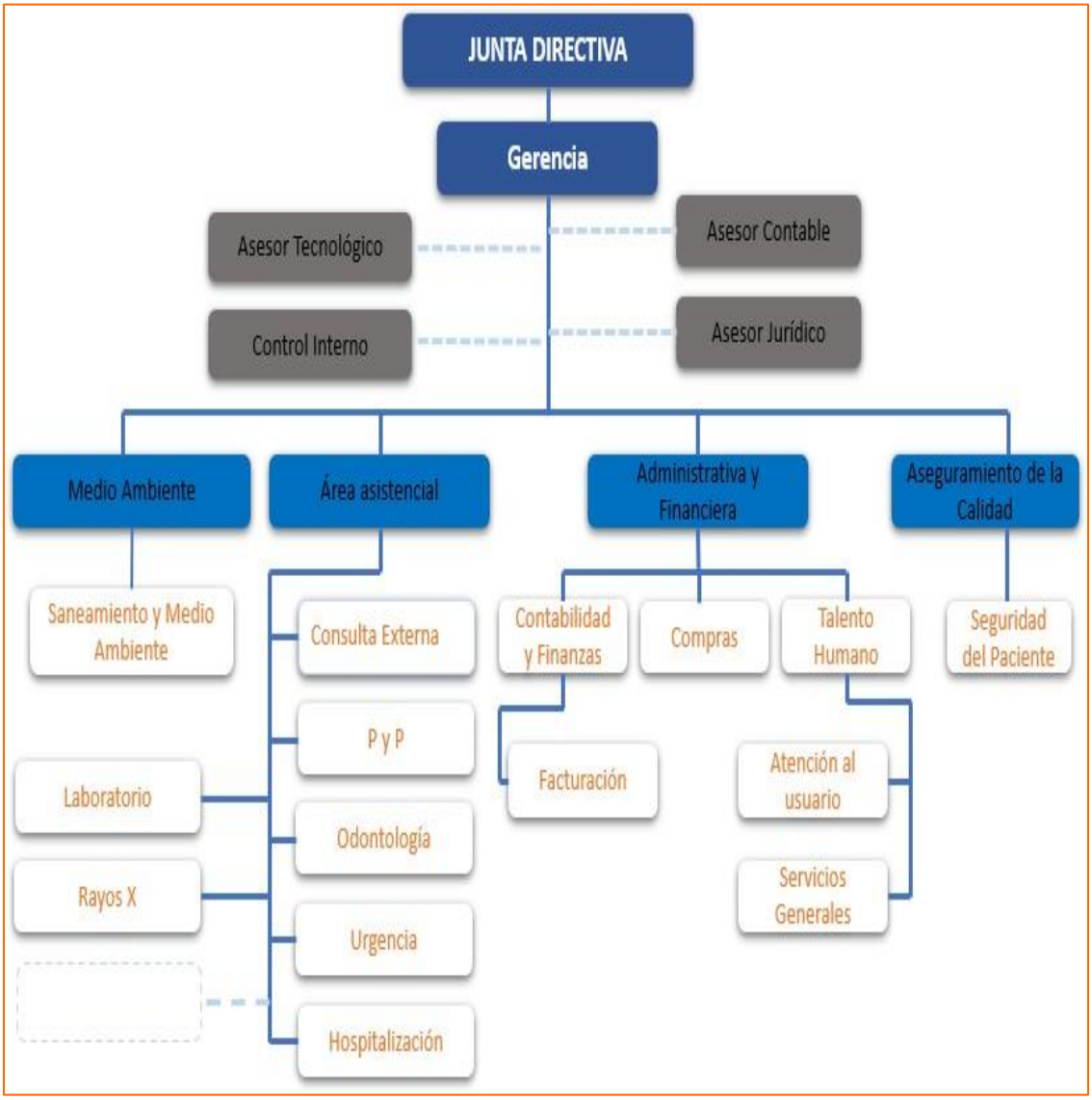
VALORES DE INTEGRIDAD



MAPA DE PROCESO



ORGANIGRAMA



POLÍTICA DE SEGURIDAD DE LA INFORMACION

Hemos realizado un listado de pautas que se deben tener en cuenta para dar un uso adecuado a los recursos informáticos (correo electrónico, red interna, internet) provisto por la entidad hospitalaria.

El área de sistemas de información revisará de manera periódica los equipos de cómputo y periféricos así como el software instalado.

El propósito de estas políticas es asegurar que los funcionarios utilicen correctamente los recursos tecnológicos que la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, pone a su disposición para el desarrollo de las funciones institucionales.

El cual todo el personal (funcionarios, personal de planta, y contratistas), de la Institución, deberá ser notificado al proceso de sistemas de información, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo)) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático. Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática.

Todo servidor o funcionario nuevo en la E.S.E Hospital Nuestra Señora del Carmen de Guamal, Magdalena, deberá contar con la inducción y en el caso de personal antiguo de una re inducción sobre las Políticas y Estándares de Seguridad Informática, donde se dan a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento. Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

SEGURIDAD FISICA Y DEL MEDIO AMBIENTE

Para el acceso a los sitios y áreas restringidas se debe notificar al proceso de sistemas de información para la autorización correspondiente, y así proteger la información y los bienes informáticos. El usuario o funcionario deberán reportar de forma inmediata al procesos de sistemas de información cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio. El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante. Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Cualquier persona que tenga acceso a las instalaciones de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de portería o facturación de urgencias, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente. Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán ser retirados de las instalaciones de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, únicamente con la autorización de salida del área de Inventarios y/o almacén, anexando el comunicado de autorización del equipo debidamente firmado por el gestor de sistemas de información.

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Oficina de sistemas de información, en caso de requerir este servicio deberá solicitarlo. El Área de Inventarios de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el proceso de sistemas de información.

El equipo de cómputo asignado, deberá ser para uso exclusivo para uso de las funciones netamente laborales. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos. Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU. Se debe mantener el equipo informático en un lugar limpio y sin humedad. El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar una reubicación de cables con el personal del proceso de sistemas de información. Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al proceso de sistemas de información a través de un plan detallado. Queda terminantemente prohibido que el usuario o funcionario distinto al personal de la sistemas abra o destape los equipos de cómputo.

Únicamente el personal autorizado por el proceso de sistemas de información podrá llevar a cabo los servicios y reparaciones al equipo informático. Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

PERDIDA DE EQUIPO

El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo. El préstamo de laptops o portátiles tendrá que solicitarse a la Oficina de sistemas de información con el visto bueno del gerente de la Institución. El servidor o funcionario deberán dar aviso inmediato al proceso de sistemas de información, y a la Administración de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

USO DE DISPOSITIVOS EXTRAIBLES

El uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de CD y DVD Externos para el manejo y traslado de información o realización de copias de seguridad o Backups deberá ser notificado al proceso de sistemas de información en caso que se trate de información sensible y/o datos de historias clínicas.

DAÑO DEL EQUIPO

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad. El cual será notificado.

CONTROLES PARA LA GENERACION Y RESTAURACION DE COPIAS DE RESPALDO (BACKUPS)

Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores. Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups. Las copias de seguridad o Backups se deben realizar al menos una vez a la semana y el último día hábil del mes.

PLANES DE CONTINGENCIA ANTE DESASTRE

Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total. El proceso de sistema de información debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre. Disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados. Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.

Existencia de documentación de los procedimientos manuales a seguir por los distintos procesos usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos. Existencia de documentación de los procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros. Existencia de documentación de pruebas periódicas de la implementación del plan de recuperación ante desastre para verificar tiempos de respuesta, capitalizando los resultados de la pruebas para el afinamiento del plan.

Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la institución. Disponibilidad de copias de respaldo para restablecer las operaciones en las áreas de misión crítica definidas.

INFORMACION SENSIBLE Y/O CONFIDENCIAL

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, debe ser proporcionado por el dueño de la información, con base en el principio de "Derechos de Autor" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones. Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el proceso de sistemas de información antes de poder usar la infraestructura tecnológica. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica, a menos que se tenga el visto bueno del dueño de la información y del

proceso de sistemas de información y la autorización de su Jefe inmediato. Cada usuario que acceda a la infraestructura tecnológica debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios. Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

VIOLACIONES DE SEGURIDAD INFORMATICA

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el proceso de sistema de información. Ningún usuario o funcionario de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el proceso de sistema de información. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la entidad hospitalaria.

EQUIPOS EN EL AREA ADMINISTRATIVA

El gestor deberá poner a disposición del proceso de sistemas de información, la información contractual de los equipos informáticos de Cómputo Escritorio, Portátil y periférica, así como de los servicios de soporte y mantenimiento. El proceso de sistema de información, será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos. El proceso de sistemas de información, tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación, mismos que serán entregados por la Alta dirección o el área usuaria de la licencia, para llevar el control de software instalado, para los equipos informáticos de cómputo Escritorio, Portátiles y periféricos al momento de la recepción de los mismos. Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el gestor o Jefe del proceso solicitante, lo cuales serán evaluados por el proceso de sistemas de información. El proceso de sistemas de información, es el área encargada de tramitar las asignaciones, reasignaciones, bajas, etc. de equipos informáticos de cómputo Escritorio, Portátiles y periféricos ante la Sección Financiera entidad encargada del Inventario de Activos para su ejecución.

Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar al proceso de sistemas de información el movimiento así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.

El proceso de sistemas de información deberá elaborar el pase de salida cuando algún bien informático de cómputo Escritorio, Portátiles y periférico requiera ser trasladado fuera de las instalaciones de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, por motivo de garantía, reparación o evento. Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida quedará a consideración del proceso de sistema de información para su autorización y visto bueno. Las diferentes Áreas de la ESE serán encargadas de proporcionar al proceso de sistemas de información, la relación de bienes y equipos que entrarán al proceso de baja, según corresponda.

El proceso de sistemas de información realizara la evaluación técnica del equipo y definirá la reasignación o baja definitiva del bien que será informada a la Sección Financiera para control de Inventarios de Activos por medio del procedimiento definido por el mismo.

Queda prohibida la baja de equipo de cómputo que no cuente con evaluación técnica por parte del proceso de sistema de información.

A los equipos portátiles personales no se les brindará soporte de ninguna índole: ni de hardware ni de software, porque no son responsabilidad de la entidad por ende el dueño debe hacerse cargo y responsable de su computador. La dirección IP asignada a cada equipo debe ser conservada y no se debe cambiar sin la autorización de la Oficina de Sistemas porque esto ocasionaría conflictos de IP'S y esto alteraría el flujo de la red.

No llenar el espacio de disco del equipo con música ni videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad.

Todo funcionario responsable de equipos informáticos debe dejarlo apagado y desenchufado tanto al medio día como en la noche lo anterior para ahorrar recursos energéticos y contribuir a la conservación de los equipos.

PERSONAL DE SEGURIDAD DE LA INFORMACION

Las funciones del personal de seguridad de la información son asumidas por los profesionales Universitarios Sistemas de información de la E.S.E.

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El plan de implementación para el componente de seguridad y privacidad de la información, corresponde al plan operativo anual establecido por la Oficina Comunicaciones y Sistemas, al cual se le hace un seguimiento mensual.

NUMERO DE ACTIVIDAD	ACTIVIDADES	ACCIONES DE MEJORAMIENTO	INDICADOR	RESPONSABLES
1	Establecer una política para la seguridad y privacidad de la información	En eras de proteger los datos personales de los usuarios y otros que reposen en el hospital, la entidad se compromete a la creación e implementación de una política de seguridad y privacidad de la información y de esta manera establecer una confianza en función de los deberes entre el estado y el ciudadano.	Lograr en un 90% la ejecución de la actividad	Control Interno, calidad,
2	Registro y actualización de base de datos	El hospital con ánimos de salvaguardar el habeas data, se compromete en adoptar y divulgar lineamientos a todos los funcionarios, contratistas y demás partes interesadas con el fin de almacenar y respaldar información y bases de datos personales de la E.S.E contenidas en medios físicos o electrónicos.	Lograr en un 86% la ejecución de la actividad	Control Interno Sistema
3	Capacitaciones de Seguridad de la información y tratamiento de	Designar a un personal capacitado para realizar capacitaciones periódicas a funcionario y contratistas de la entidad, con el fin de	Lograr en un 87% la ejecución de la actividad	Personal encargado Sistemas Control Interno

	datos personales	proporcionar información y actualizaciones con respecto a temas ofimáticos y tratamiento de base de datos físicos y electrónicos		
4	Procedimiento de Backup de información de bases de datos personales digitales.	A través de una política enfocada a la protección de datos, implementar un proceso de Backus o respaldo de copias de seguridad de los datos originales que reposan en archivos digitales o conjunto de software de la entidad que se almacene en un lugar seguro o región segura de la memoria del sistema.	Lograr en un 89% la ejecución de la actividad	Sistemas
5	Procedimiento de respaldo y almacenamiento de base de datos personales físicas	Realizar procesos de respaldos de bases de datos personales físicos, que permite mantener una copia y proporcionar información a las partes interesadas y quien la requiera	Lograr en un 87% la ejecución de la actividad	Sistemas Calidad
6	Procedimiento de asignación de contraseñas a equipos de computo	Realizar un procedimiento o capacitar al personal para la correcta asignación de contraseñas a los equipos de cómputo de la entidad, con el fin de proteger los datos ofimáticos de los responsables de los equipos	Lograr en un 98% la ejecución de la actividad	Sistemas