1. RESPONSABLE

El responsable de llevar a cabo este plan es el Líder de Sistemas.

2. OBJETIVO

Involucrar a todo el personal para el manejo adecuado y utilizar las mejores prácticas para el manejo de la información aplicando el concepto de seguridad digital.

Supervisar la información vital de la empresa y realizar los procedimientos pertinentes para que no se pierda y/o alterada.

3. ALCANCE

El presente plan abarca todas las instancias del Hospital sin importar que sean del área administrativa, financiera o asistencial

4. DEFINICIONES

Backup: se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos. La forma verbal es hacer copias de seguridad en dos palabras, mientras que el nombre es copia de seguridad.

Antivirus: Es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

Medio magnético: Es un dispositivo que almacena la información en por medio de ondas magnéticas. Son medios magnéticos los discos duros, discos de 3 1/2″, cintas de audio o casetes. Como medida de protección de los medios magnéticos se deben realizar de copias de seguridad y resguardo.

Historias clínicas: Es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención.

Contraseña: Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

Correo electrónico: es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos. ... La explicación es sencilla: @, en inglés, se pronuncia at y significa “en”.

Hardware: Es la parte física de un ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y circuitos de luz, placas, utensilios, cadenas y cualquier otro material, en estado físico, que sea necesario para hacer que el dispositivo funcione correctamente.

Software: Al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

IP: Es la sigla de Internet Protocolo, en nuestro idioma, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. El IP no cuenta con la posibilidad de confirmar si un paquete de datos llegó a su destino.

Sistemas de información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

5. REF NORMATIVA

Decreto 612 del 4 de abril de 2018.

6. DESARROLLO

FORMULACIÓN DEL PLAN:

La ESE Hospital Geriátrico y Ancianato San Miguel cuenta con un plan estratégico de la tecnología y comunicaciones y el plan de tratamiento de riesgos de seguridad y privacidad de la información contemplado como contingencia el cual aporta las herramientas necesarias que aportan al presente plan en todo lo relacionado con la seguridad y privacidad.

HERRAMIENTAS DE APOYO:

Contamos con procedimientos para garantizar la seguridad y privacidad de la información que indicaremos a continuación:

- Se realizan Backups automatizados en medios magnéticos para salvaguardar la información contable y administrativa de la ESE.
- Se realiza levantamiento de información de manera semanal la información que contienen Historias clínicas salvaguardadas en un storage en la nube.
- Se realiza backups diarios en el área presupuestal y son almacenados en el storage externo.
- La información vital de las estaciones de trabajo es almacenada en medios magnéticos y alojadas en el área de gestión documental.

ACTIVIDADES

A continuación, se indicarán las diferentes tareas preventivas que se desarrollan para los respaldos de la información:

- Los paquetes contables utilizados en la ESE Hospital Geriátrico y Ancianato San Miguel como el software SIESA (CGuno) se realiza backup de su base de datos todos los días en medios magnéticos. Cuando este medio magnético se llena toda esa base de datos es alojada en la nube para tener 2 backups de respaldos.
- El paquete presupuestal manejado con el software GEMA es almacenado de manera diaria en la nube de la empresa y se almacena otra copia en el equipo donde se realiza el procedimiento.
- Los usuarios que manejan información tangible del hospital como estadística, contabilidad, se realiza almacenamiento de datos mensualmente en medios magnéticos.
- Todos estos archivos con sus medios magnéticos son llevados y guardados en el área de gestión documental de la ESE.
- Se realiza supervisión de los respaldos realizados tomando aleatoriamente cualquier backup y montándolo en el sistema para verificar la información.

DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACCESO A LA INFORMACIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la ESE siendo este el activo más importante, su manejo influye en el objetivo de alcanzar la misión institucional y está expuesta a problemas de seguridad, por consiguiente, debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos y contribuyendo de esta manera, a una mejor.

Todos los funcionarios que laboran para la ESE deben tener acceso sólo a la información necesaria para el desarrollo de sus funciones. Las herramientas y accesos otorgados para el uso de los sistemas de información de la entidad, servicios de red y correo deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios.

Toda la información contenida, procesada o generada en los equipos de cómputo es propiedad de la ESE Hospital Geriátrico y Ancianato San Miguel. Los funcionarios que laboran en la ESE, son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la entidad y por la normativa que la proteja, tendiente a evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. Entre esta información tenemos la siguiente: hojas de Excel, documentos tipo Word, documentos tipo PowerPoint, correo electrónico, PDF, entre otros.

Todos funcionarios que utilice los recursos informáticos tienen la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y crítica.

No se debe dejar visible sus contraseñas de correo, red y archivos, porque pueden ser utilizadas por otras personas alterando o dañando su información, ni tampoco comparta sus contraseñas pueden ser utilizadas con otros objetivos.

No debe permitir que personal externo opere su información.

Al desplazarse de su puesto de trabajo, bloquee la sección en el equipo, esto evita posibles ingresos no autorizados a su información.

SEGURIDAD SISTEMAS DE INFORMACIÓN

El software contable (SIESA), aplicativo de presupuesto (GEMA), historias clínicas (RFAST), herramientas ofimáticas, son utilidades asociadas de la entidad que debe ser usado únicamente para el ejercicio de las funciones y actividades de competencia de cada usuario.

El uso de la red Internet debe ser solo para fines laborales, no está permitido el ingreso a páginas del siguiente tipo: pornografía, radio y tv, juegos, armas, sitios maliciosos, software free, entre otros.

CONTRASEÑAS

La contraseña debe de cumplir con una longitud mínima de 8 caracteres, y al menos con tres tipos entre los caracteres siguientes: ✓ Letras Mayúsculas ✓ Letras Minúsculas ✓ Números en sustitución de letras (1 por I, 0 por o, 3 por la E, etcétera) ✓ Caracteres especiales no alfanuméricos, como signos de puntuación ✓ Cada 42 días el sistema le exige que cambie su contraseña en el área asistencial.

SEGURIDAD EN RECURSOS INFORMÁTICOS

Todos los recursos informáticos deben cumplir con lo siguiente:

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos y da parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiarlas y los períodos de vigencia de las mismas, entre otras.

Todo sistema de información debe tener definidos los perfiles de usuario de acuerdo con la función y cargo que puedan acceder a dicho sistema.

Toda la información que sea sensible, crítica o valiosa debe tener controles de acceso para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

SEGURIDAD EN COMUNICACIONES

Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información confidencial.

SOFTWARE UTILIZADO

Todo software que utilice la ESE será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Todo el software de manejo de datos que utilice la ESE dentro de su infraestructura informática deberá contar con las técnicas más avanzadas para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la entidad que garantice el conocimiento por parte de los usuarios, contratistas y practicantes de las implicaciones que tiene el instalar software ilegal en los computadores.

La instalación de software en Los equipos de cómputo estará controlada mediante configuración especial en dichos computadores, la cual solicitará usuario y contraseña del administrador al momento de realizar una instalación, esto asegura que ningún programa o Software podrá ser instalado en los computadores

ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del personal de sistemas. La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal del personal de sistemas y se documentará cuando no exista garantía vigente de las partes a reemplazar. Los computadores e impresoras no deben reubicarse sin la aprobación previa del personal de Sistemas.

ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de la ESE Hospital Geriátrico y Ancianato San Miguel deberá ser almacenada y respaldada de acuerdo con las buenas prácticas de TI de tal forma que se garantice su disponibilidad.

Cada usuario tiene asignado un acceso en el storage de la nube de acuerdo con el proceso que pertenece, toda información que sea generada por sus funciones en la ESE debe ser almacenada en dicho almacenamiento y no en otro lugar, ya que estos recursos son los que se les aplica las copias de seguridad.

Los usuarios son responsables de la información en los computadores, siguiendo las indicaciones técnicas dictadas por el personal de sistemas.

El personal de sistemas define la estrategia a seguir para el respaldo de la información.

La información de tipo audio, video, imágenes y archivos personales, no están permitidos en los recursos de almacenamiento dispuestos por la ESE.

PROGRAMACIÓN DE COPIAS DE SEGURIDAD

En la ESE Hospital Geriátrico y Ancianato San Miguel se tienen programadas las copias de seguridad de la siguiente manera:

- Mensual (Abuelo): corresponde a los datos que se generan durante el mes y el medio de almacenamiento de dicha información es en medio magnético la cual esta custodiada en el área de Gestión Documental.
- Semanal (Padre): corresponde a todo el dato generado en la semana, el medio de almacenamiento es en la nube, es una copia completa de archivos.
- semana. Diaria (Hijo): corresponde a todos los datos generados en el día, el medio de almacenamiento es en la nube. Se realiza de lunes a viernes.

PROTECCIÓN CONTRA VIRUS

El virus por computador puede definirse como un programa con capacidad de reproducir un error (infección) e insertarlo en las áreas de datos, de programas del mismo sistema y alterar su normal funcionamiento. Estos atacan destruyendo la integridad de la información contenida en los medios de almacenamiento magnético llegando incluso a dañar partes físicas de la máquina. Aunque existe software antivirus, lo primordial es prevenir el contagio mediante la adopción de una política de sano procesamiento que el usuario debe seguir: Hacer un escaneo con el servicio de antivirus institucional a todo documento, imagen, video, medio magnético, descargas online, adjuntos de correo electrónico; previniendo el ingreso de virus informática y demás riesgos que esto contrae. Utilizar únicamente software autorizado e instalado por el auxiliar administrativo en sistemas e informática. Cada equipo de la ESE cuenta con el software de antivirus con la empresa AVG Internet Security teniendo herramientas de protección como la verificación de archivos en tiempo real, protección en la web y correo electrónico, ataques de hackers, privacidad de la información y pagos protegidos.

HARDWARE

- El equipo de cómputo será asignado de acuerdo con el puesto o función laboral en su proceso.
- Cada equipo está preparado con el hardware y software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y lógico del mismo incluyendo sus periféricos.
- En caso de presentar una falla física o lógica se deberá notificar al área de sistemas e informática.

- En ningún caso el usuario intentara reparar el equipo o diagnosticarlo, únicamente informar de la posible falla.
- El usuario será el único responsable del equipo de cómputo.
- Solo se utilizará el equipo para funciones de interés de la ESE y de ninguna manera para asuntos personales.
- Cada equipo contiene el software de acuerdo con las necesidades del proceso.
- Por ningún motivo el usuario instalara software de promoción y entretenimiento.
- La adquisición o desarrollo de software será responsabilidad del área de sistemas e informática.

PAUTAS PARA EL USO AUTORIZADO DEL CORREO ELECTRÓNICO

El servicio de correo electrónico de la ESE, está habilitado exclusivamente para apoyar la gestión misional y administrativa de la entidad. Esto significa que el funcionario o persona autorizada utiliza este servicio para los propósitos de misión y razón de ser de la ESE y la comunicación con entidades, empresas, proveedores, clientes y contratistas.

Las siguientes son provisiones específicas con respecto al uso autorizado del buzón de correo electrónico que se asigna a un funcionario o persona autorizada dentro de la ESE Hospital Geriátrico y Ancianato San Miguel:

RECOMENDACIONES Y USOS AUTORIZADOS

Los buzones de correo electrónico tienen un tamaño de 100GB para todos los funcionarios, este servicio se encuentra disponible en la nube el hosting ancianatosanmiguel.com y es responsabilidad del usuario velar por la seguridad del ingreso a la plataforma fuera de las instalaciones de la ESE.

Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.

Se permite la suscripción a listas de distribución y otras formas de los servicios de la suscripción del correo electrónico relacionados con la función del trabajo.

El uso del correo electrónico como recurso institucional asignado debe manejarse con conducta ética y responsable, acatando el mandato legal vigente relacionado con el uso de recursos tecnológicos o cualquier otra regulación interna expedida en este sentido por la entidad.

USO PROHIBIDO DEL CORREO ELECTRÓNICO

Los funcionarios o personas autorizadas de la ESE no utilizaran el servicio de correo electrónico para crear, ver, guardar, recibir, o enviar material de los siguientes casos:

- No utilizar la cuenta de correo electrónico institucional, en redes sociales como Facebook, Instagram u otro tipo de red que envié notificaciones o información al buzón que no tiene nada que ver con la ESE.
- Crear o intercambiar mensajes ofensivos u obscenos de cualquier clase, incluyendo material pornográfico.
- Enviar correo electrónico que contenga amenazas o mensajes violentos.
- Intercambiar mensajes con información confidencial con alguien externo y ajeno a la ESE.
- Creación, reenvió o intercambio de mensajes SPAM (correo no solicitado), cadenas de cartas, solicitudes o publicidad.
- Crear, almacenar o intercambiar mensajes que contengan material protegido bajo las leyes de derechos de autor, sin el consentimiento de su(s) autor(es).
- Divulgar mensajes con datos o información institucional no autorizada.
- Divulgar sus contraseñas de correo.
- Alterar el contenido del mensaje de otro usuario sin su consentimiento.
- Utilizar como propia la cuenta de correo de otro funcionario sin su permiso.
- Inscribir la cuenta de correo en listas no relacionadas con la gestión de la ESE.
- Borrar mensajes cuyo contenido es relevante o importante, dentro de las funciones asignadas como funcionario o para la entidad.
- Enviar mensajes con archivos anexos extensos, que puedan afectar el desempeño del servicio y de la red local.

PRIVACIDAD

Los funcionarios, usuarios o personas autorizadas no deben mantener expectativa de privacidad, mientras estén usando el correo electrónico de la ESE Hospital Geriátrico y Ancianato San Miguel; Además, la información que transite temporalmente o se almacene de manera permanente en los recursos informáticos de la ESE será monitoreada, la ESE mantendrá el derecho de monitorear y revisar el contenido enviado o recibido por los funcionarios a través del servicio de correo electrónico, cuando sea necesario, tales comunicaciones no deben ser consideradas como privadas o seguras.

VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD

Las siguientes actividades son consideradas como violaciones a las políticas de seguridad:

- Enviar correo electrónico no solicitado o Spam.
- Envío de correo con contenidos pornográficos.
- Instalación o ejecución de software no autorizado.
- Utilización del internet indebidamente, esto incluye, navegación a páginas con contenidos pornográficos, sitios de música en línea, juegos en línea, sistemas de mensajería instantánea (no autorizados), casinos, proxys piratas, programas de carga de archivos, o cualquier otro sitio con fines diferentes a los laborales.

- Traslado o instalación de nuevos equipos a la red sin la autorización ni el procedimiento establecido por el proceso de recursos tecnológicos.
- Dañar física o lógicamente los equipos o la infraestructura informática.
- Instalar dispositivos o tarjetas de acceso remoto, módems. RDSI, routers o cualquier otro dispositivo de comunicaciones en los clientes de la red.
- Utilizar cualquiera de los recursos informáticos de la ESE para fines diferentes a las funciones contractuales, ya sea funcionario o contratista.
- Utilizar cualquier tipo de software para fines malicioso o intrusos tales como sniffers, port scanner, keyloggers, entre otros.
- Utilizar cualquier técnica de hacking hacia cualquiera de los recursos tecnológicos de la ESE entre los que se incluye, ataques DoS, phising, spoofing y broadcast storm.
- Violación o cambio de contraseñas diferentes a las personales.
- Usar cuentas de equipos sin autorización.
- Conseguir acceso no autorizado a cualquier equipo o información.
- Conseguir acceso no autorizado a los recursos compartidos, almacenados en los equipos y servidores de la infraestructura informática.
- Acceso sin autorización a equipos de red tales como servidores, routers, Switches, Access Point, Firewalls, u otros elementos de la red o que estén en sus instalaciones.
- Ejecución intencionada de scripts que comprometan la seguridad y buena utilización de los recursos.
- Ejecutar una base de datos con el propósito de colectar datos contenidos en ella.
- Acceso no autorizado a sistemas críticos y delicados como sistema contable, software de presupuesto, historias clínicas y unidad de red no autorizada.
- Realizar o modificar transacciones indebidas en cualquier sistema financiero implementado en la ESE.
- Ejecución de comandos SNMP a servidores de correo.
- Utilizar cualquiera de los recursos informáticos de la ESE para fines lucrativos diferentes a los contratos.
- Las violaciones de las políticas de seguridad y privacidad por parte de funcionarios y contratistas o usuarios de los recursos tecnológicos darán lugar a la respectiva investigación de carácter disciplinario, penal, civil y fiscal a que haya lugar.

PROPIEDAD INTELECTUAL

La ESE Hospital Geriátrico y Ancianato San Miguel, por medio del área de sistemas podrá tener acceso en el momento que sea necesario a cualquier información alojada en alguno de los equipos que son propiedad del mismo tales como PC, servidores, almacenamiento en la nube entre otros, así mismo podrá tener acceso a cualquier información generada y transmitida por la red. Todos los computadores y servidores de la ESE deberán pertenecer al grupo de trabajo denominado HGASM y sujetarse a las políticas de seguridad que estén establecidas actualmente, por lo tanto, cualquier software que se esté instalando en las

maquinas deberá tener su respectiva licencia y previa autorización por parte del área de sistemas e informática para su correcto funcionamiento.

Todas las contraseñas y accesos de los usuarios sean contratistas o de planta son creadas y salvaguardadas por el área de sistemas de la ESE. Si el usuario va realizar modificaciones sobre las contraseñas debe diligenciar el formato GIC-SIS-for-001 para su respectivo cambio.

7. ANEXOS

N.A

8. APROBACION

	ELABORO	**REVISO**	**APROBO**
Nombre	MAURICIO GOMEZ	ARIADNA BOLAÑOS	HECTOR FABIO CORTES
Cargo	Lider Sistemas	Responsable Planeación	Gerente