POLÍTICAS DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

Objetivo

- La E.S.E. HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO – HUILA a través del trabajo en equipo con sus funcionarios deben garantizar la protección de toda la información generada, procesada y resguardada por los sistemas de información y su infraestructura tecnológica.

Alcance/Aplicabilidad

- Éstas Políticas aplican a toda la entidad, sus funcionarios, terceros, aprendices, practicantes, proveedores de la E.S.E. HOSPITAL DEPARTAMENTAL SANANTONIO DE PITALITO - HUILA y la ciudadanía en general.

Nivel de Cumplimiento

- Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% a las presentes políticas.

1. Escritorio Limpio y Bloqueo de Sesión

a) Durante el día: Guarde los documentos sensibles bajo llave.

b) Si utiliza un computador portátil, manténgalo en un lugar seguro para evitar robos.

c) No deje USB's, CD's, u otro elemento removible con información en lugares visibles y accesibles.

d) Guarde su portafolio o cartera en muebles seguros.

e) No deje accesible documentos impresos que contengan datos sensibles, por ejemplo: Datos de empleados, contratos, números de cuenta, informes confidenciales, información de propiedad intelectual, nombres de usuarios y Passwords (claves).

f) Siempre al levantarnos de nuestro puesto de trabajo debemos bloquear nuestro equipo de cómputo, para evitar que otras personas puedan acceder a nuestra información:

- Debemos Pulsar simultáneamente (el Botón de inicio + la tecla L) para bloquear nuestro equipo.
- Pulsar (Ctrl + alt + supr) y seleccionar la opción bloquear equipo.

- Al regresar introducimos nuevamente nuestra contraseña para continuar trabajando.

g) Al terminar el día tómese unos minutos para:

- Juntar y guardar en forma segura el material sensible. Cerrar con llave gabinetes, cajones y oficinas.
- Asegurar el equipo costoso (Portátiles, Celulares, etc.).
- Destruir de forma efectiva los documentos sensibles.

2. Manejo Apropiado de las Impresiones

Es importante tener presente las siguientes recomendaciones para el manejo de impresiones de documentos:

a) Las impresoras solo podrán ser utilizadas para imprimir documentos requeridos por la institución.

b) Retirar los documentos que se envían a imprimir.

c) Todo documento que quede en la impresora al final del día, debe ser eliminado.

d) En caso del mal funcionamiento en una impresora, o que está siendo mal utilizada, deberá informar al área de Sistemas.

e) Cada área será la responsable de mantener los suministros correspondientes.

f) El material impreso que contenga información sensible debe:

- No dejarlo descuidado en áreas abiertas
- Ser removido de las impresoras sin demora

g) Los impresos como cheques, certificados, etc, deben ser almacenados en forma segura y sólo proporcionados al personal autorizado.

3. Manejo Apropiado De Contraseñas

Consejos:

a) Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
b) Las contraseñas se deben mantener confidenciales en todo momento.

c) No compartir las contraseñas, con otros usuarios.
d) Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso a ésta.
e) Selecciona contraseñas que no sean fáciles de adivinar.
f) Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre-definido.
g) Cambia tus contraseñas regularmente.
h) No utilizar la opción de almacenar contraseñas en Internet.
i) No utilizar contraseña con números telefónicos, nombre de familia etc.
j) No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

Para crear una contraseña se debe tener en cuenta:

- Contraseñas fuertes contienen números y letras. Ver tabla adjunta.
- Utilizar contraseña que tengan por lo menos 8 caracteres

Categoría de Caracteres	Ejemplos
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' <> , . ?

4. Manejo Apropiado de Control de Virus

La E.S.E. Hospital Departamental San Antonio de Pitalito, ha definido como producto estándar Kaspersky Antivirus, en entorno de estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computacionales.

a) El sistema de actualizaciones y detección diaria es automatizado a nivel central.

b) El área de Sistemas de Información será la única autorizada para instalar, activar, desactivar, y desinstalar el programa de Antivirus Insitucional (Kaspersky).

c) Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus al área de Sistemas.

d) Los usuarios no deberán desinstalar el producto de antivirus existente en su equipo.
e) Los dispositivos extraíbles antes de ser usados deben, realizar scanner con el antivirus.

5. Manejo de Cuentas de Sistemas

a) Toda cuenta de acceso que se requiera modificar deberá ser solicitada a través de los administradores de los sistemas.

b) El procedimiento de creación de cuentas, debe ser canalizado a través de la Oficina de Sistemas de Información.

c) Cuenta de red: Esta cuenta corresponde a la que utilizará cada usuario para conectarse a su equipo PC.

d) Cuenta de Correo interno y mensajería instantánea: Se debe solicitar de manera formal a la Oficina de Sistemas de Información.

e) Cuenta de Índigo Crystal y Dinámica Gerencial: Debe ser solicitada a la Oficina de Sistemas de Información, previa autorización de la Oficina de Talento Humano.

La eliminación de cuentas se realizará de manera formal a través de un listado de las personas que no continúan vinculadas a la institución, certificada por la Oficina de Talento Humano.

6. Manejo de Acceso a Internet

El acceso a internet se encuentra protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio. Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

- No está permitido:

a) Navegar por sitios no confiables.

b) El uso de sitios de radios online.

c) El uso de intercambio de archivos (Ares, eMule, Torrents, Limewire, etc.).

d) El uso de sitios de chat (Messenger, chat, etc.).

e) El uso de internet para actividades ilícitas.

f) La descarga que no cumpla con la normativa vigente de copyright y similar.

g) El acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

h) Compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo, etc).

i) Que el navegador de internet recuerde la contraseña automáticamente.

j) Participar en juegos de entretenimiento en línea.

k) Dejar las ventanas abiertas del navegador cuando no se está navegando por internet.

l) Recibir, descargar, y abrir cualquier archivo de internet sin previamente haber sido escaneado por el antivirus institucional, para asegurar que no tenga virus.

La Oficina de Sistemas de Información queda facultada para suspender el servicio de navegación en internet bajo circunstancias que así lo requiera (Virus, mal uso de internet, trafico sospechoso, etc.).

Si se requiere navegar en algún sitio bloqueado se debe enviar la solicitud vía email (Correo externo: sistemas@hopitalpitalito.gov.co. Correo interno: ftrujillo@hsanpitalito.local) en el formato Solicitud de Permisos de Seguridad HSP-SI-F10, para su análisis y aprobación.

7. Manejo de Correo Electrónico Institucional (Interno y Externo)

La Oficina de Sistemas de Información cuenta con filtros para identificar y bloquear correos no deseados (Spam o Virus).

- Uso Adecuado del Correo Electrónico (Interno y Externo):

a) El Correo electrónico es de uso exclusivo para trabajos de La E.S.E. Hospital Departamental San Antonio de Pitalito y queda restringido el uso para otros fines.

b) Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que atente contra las buenas costumbres o principios éticos, como: Material pornográfico, difamatorio, racista, contenido multimedia (música, videos, imágenes, entre otros).

c) Todo correo ajeno que no pertenezca a la E.S.E. Hospital Departamental San Antonio de Pitalito, no se entregará soporte técnico e informático por el área de Sistemas de Información.

d) Debe ser cambiada la contraseña de correo periódicamente.

e) En el desarrollo de actividades institucionales, reporte de información a las diferentes entidades y/o entes de control, en las cuales se solicita el correo electrónico, se debe suministrar el correo electrónico institucional de la respectiva área y/o servicio.

f) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por La E.S.E. Hospital Departamental San Antonio De Pitalito y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

g) No pichar link sospechosos llegados por correos electrónicos (bancos, tiendas, etc.).

h) No completar datos personales en correos electrónicos sospechosos.

i) Eliminar correo no deseado (Spam o sospechoso).

j) No enviar correo cuyos archivos superen los 5MB.

8. Manejo de Redes Sociales

La Oficina de Sistemas de Información bloquea todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiere acceder a ello, el coordinador del área administrativa ó del área asistencial debe enviar la solicitud formal a la Oficina de Sistemas de Información, mediante el diligenciamiento del formato Solicitud de Permisos de Seguridad HSP-SI-F10, para su análisis y aprobación.

Cabe destacar que cualquier imagen, foto, archivo y/ o comentario cargado en algunas de las redes sociales (Facebook, Twitter, Youtube, Flickr, Skype, Linked in, Instagram, entre otras) es responsabilidad exclusiva de quien la emite.

9. Manejo de Software

- No está permitido:

a) La instalación de software que no cumpla con la normatividad vigente en materia de derechos de autor, que su procedencia sea dudosa, que no esté licenciado y que no haya sido autorizado por la Oficina de Sistemas de Información.

b) Que los usuarios descarguen e instalen aplicaciones, que puedan provocar alguna vulnerabilidad o inestabilidad en los sistemas de información del Hospital.

Todo requerimiento de instalación de un nuevo aplicativo y/o software debe ser canalizado a través del Formato Solicitud de Permisos de Seguridad HSP-SI-F10 (Manual de Procesos y Procedimientos de Seguridad de la Información HSP-M08 de 2013), para su análisis y aprobación.

10. Manejo de Dispositivos Móviles (Celulares, Smartphones, PDAs, Tablets, otros)

Para garantizar la seguridad de la información, la estabilidad y la capacidad de navegación de la red interna y externa; así como el uso de los dispositivos móviles (Provistos por el Hospital y de Terceros) al interior del Hospital; se reglamenta su uso bajo los siguientes lineamientos:

- Dispositivos Móviles Institucionales:

a) Los teléfonos móviles de la E.S.E. Hospital Departamental San Antonio de Pitalito son de uso exclusivamente para facilitar el desarrollo de actividades laborales de la entidad.

b) En caso de licencia, vacaciones o retiro definitivo del funcionario que tenga a cargo un dispositivo móvil, éste debe quedar a disposición del área y/o servicio al que fue asignado.

c) La instalación, configuración, modificación o eliminación de software en los dispositivos móviles es responsabilidad exclusiva de la Oficina de Sistemas de Información.

d) No descargar ningún software que no se encuentre licenciado o que indique claramente que es de licencia libre.

e) Las actualizaciones de sistemas operativos de los dispositivos móviles, debe ser coordinadas con el área de Sistemas de Información.

f) Se debe mantener desactivada la red Wifi, Bluetooth, Infrarrojos, etc, cuando no se esté utilizando.

g) Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el teléfono móvil. Si no está seguro del proceso debe comunicarse con el Área de Sistemas de Información.

h) En caso de daño o pérdida del dispositivo móvil se debe reportar de forma oportuna a su Jefe Inmediato.

i) Se debe solicitar al área de Sistemas de Información la configuración de los correos electrónicos institucionales.

j) No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

k) No acceder a los enlaces solicitados a través de SMS, MMS, Email; para evitar código malicioso.

l) No acceder con los dispositivos móviles a las áreas restringidas y en aquellas donde funcionen equipos biomédicos (Sala de Partos, Quirófanos, Reanimación, U.C.I, Laboratorio, Imagenología, otros).

- Dispositivos Móviles No Institucionales (Funcionarios y Terceros)

a) Únicamente los funcionarios y terceros autorizados por la Oficina de Sistemas de Información, previa solicitud escrita por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica del Hospital, cumpliendo con los protocolos y herramientas de seguridad autorizados y establecidos.

b) No acceder con los dispositivos móviles a las áreas restringidas y en aquellas donde funcionen equipos biomédicos (Sala de Partos, Quirófanos, Reanimación, U.C.I, Laboratorio, Imagenología, otros).

11. Manejo de Computadores Portátiles

Para garantizar la seguridad de la información, la estabilidad y la capacidad de navegación de la red interna y externa; así como el uso de los Computadores Portátiles (Provistos por el Hospital y de Terceros) al interior del Hospital; se reglamenta su uso bajo los siguientes lineamientos:

- Computadores Portátiles Institucionales:

a) Todo computador portátil debe ser incorporado al dominio de la E.S.E. Hospital Departamental San Antonio de Pitalito, a través del protocolo establecido por la Oficina de Sistemas de Información.

b) Los computadores portátiles de la E.S.E. Hospital Departamental San Antonio de Pitalito son de uso exclusivamente para facilitar el desarrollo de actividades laborales de la entidad y en especial aquellas relacionadas con el área y/o servicio al cual ha sido asignado.

c) Los equipos portátiles deben permanecer en las instalaciones de la E.S.E. Hospital Departamental San Antonio de Pitalito, durante los días y horarios hábiles de trabajo, pueden salir de las instalaciones previa autorización de Almacén y con fines institucionales.

d) En caso de licencia, vacaciones o retiro definitivo del funcionario que tenga a cargo un computador portátil, éste debe ser devuelto y quedar a disposición del área y/o servicio al que fue asignado y tramitar el respectivo paz y salvo con el Almacén cuando aplique.

e) La instalación, configuración, modificación o eliminación de software aplicativo sobre los equipos portátiles es responsabilidad exclusiva de la Oficina Sistemas de Información.

f) La Oficina Sistemas de Información deberá remover, sin necesidad de notificar al

funcionario cualquier software que no esté autorizado por la Oficina de Sistemas de Información.

g) La configuración, eliminación, modificación o cambio de sistema operativo es de responsabilidad de la Oficina Sistemas de Información

h) La configuración e instalación de hardware de los equipos portátiles, es responsabilidad exclusiva de la Oficina Sistemas de Información.

i) Se debe mantener desactivada la red inalámbrica cuando no se esté utilizando.

j) Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el equipo portátil. Si no está seguro del proceso debe comunicarse con el Área de Sistemas.

k) En caso de daño o pérdida del computador portátil se debe reportar de forma oportuna a su Jefe Inmediato.

l) No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

- Computadores Portátiles No Institucionales (Funcionarios y Terceros)

Únicamente los funcionarios y terceros autorizados por la Oficina de Sistemas de Información, previa solicitud escrita por parte de la dependencia que lo requiera, pueden conectarse a la red de datos del Hospital, cumpliendo con los protocolos y herramientas de seguridad autorizados y establecidos.