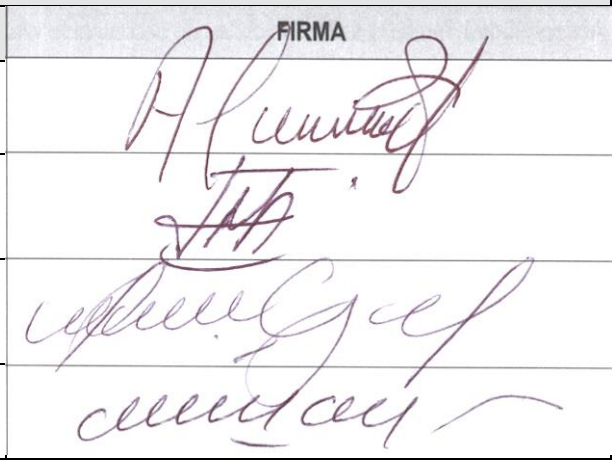
1. APROBACIÓN

	CARGO	FECHA	FIRMA
ELABORO	LÍDER DE PROCESO GESTIÓN DE LA INFORMACIÓN	19/05/2016	
APROBO	DIRECTOR ADMINISTRATIVO (E)	23/05/2016	
	COORDINADOR DE CALIDAD	23/05/2016	
	GERENTE (E)	23/05/2016	

2. OBJETIVO

Proveer a los usuarios internos de la E.S.E. Hospital Universitario de la Samaritana una herramienta de consulta que promueva la Seguridad Informática, estableciendo medidas de uso aceptable de los sistemas, técnicas y organización de las tecnologías de información, y de las personas que interactúan haciendo uso de los servicios informáticos que se proporcionan, contribuyendo con la función informática a la mejora y complimiento de metas institucionales; garantizando la Integridad, la Confidencialidad, la Disponibilidad y la Irrefutabilidad de la información.

3. ALCANCE

DESDE: Las políticas y estándares de seguridad informática, establecer medidas y patrones técnicos de administración equipos de cómputo, página web, intranet.
HASTA: La difusión sobre las políticas y estándares de seguridad informática a todo el personal de Hus Facilitando integridad, confidencialidad y confiabilidad de la información generada por la Subdirección de sistemas sobre el manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos y garantizando el buen uso de los recursos informáticos.
APLICACIÓN: Es aplicable a los usuarios de servicios de tecnologías de información de la E.S.E. Hospital Universitario de la Samaritana, incluyendo a los usuarios de programas adscritos, estudiantes universitarios y terceros o contratistas que utilicen directa o indirectamente los recursos informáticos que provee la E.S.E. Hospital Universitario de la Samaritana.

4. DEFINICIONES:

Accesibilidad: Indica la facilidad con la que el contenido Web puede ser utilizado, visitado o accedido en general por los usuarios del hospital.

Administrador de Contenidos: Sistema que permite la actualización y mantenimiento de contenidos de páginas Web. Consiste en una interfaz que controla una o varias bases de datos donde se aloja el contenido del sitio

Antispam: control anti-spam y de seguridad de correo electrónico Software que bloquea el spam y el malware a nivel de conexión mediante la comprobación de la reputación del remitente contra una base de datos dinámica de direcciones IP maliciosas conocidas.

Antivirus: Software que detecta y elimina virus informáticos, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlo para prevenir una infección por los mismos.

Buscador: Programa que realiza búsquedas en Internet de palabra o frase determinadas y como resultado proporciona un listado de sitios Web en los que se mencionan temas relacionados con la palabra o frase clave buscada.

Correo electrónico: Es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente mediante sistemas de comunicación electrónicos. Su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

Filtro de Contenido: En Informática, un filtro de contenido se refiere a un programa diseñado para controlar que contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web y aplicativos Web. (Aplication and Url Filtering Checkpoint).

Internet: Es una red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP.

Ips: Del Ingles Intrusión Prevention System, proporcionando una protección completa contra la red de tráfico de red malicioso y no deseado, incluyendo los ataques de malware, ataques DoS y DDoS, Servidor de aplicaciones y vulnerabilidades, Las amenazas internas, el tráfico de aplicaciones no deseadas, incluyendo la mensajería instantánea y P2P.

Malware: Del inglés malicious software, también llamado badware: software malicioso o software malintencionado; es un software que tiene como objetivo infiltrarse en el sistema y dañar el computador sin el conocimiento de su dueño, con finalidades muy diversas.

Moodle: Sistema de gestión de cursos, de distribución libre, que ayuda a los educadores a crear comunidades de aprendizaje en línea.

Navegador: Es una aplicación que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente en formato HTML, desde servidores Web de todo el mundo a través de Internet. Además permite mostrar o ejecutar: gráficos, secuencias de video, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces.

4. DEFINICIONES:

Página Web: Archivo que constituye una unidad significativa de información accesible en la www a través de un navegador. El Sitio Web está habitualmente creado como un conjunto de páginas, a las cuales se accede mediante enlaces.

PC: Computador personal u ordenador personal (en inglés, Personal Computer o PC) es un microcomputador, diseñado en principio para ser usada por una sola persona a la vez.

Peso de un elemento: El peso de un elemento, en el contexto de Internet, se refiere al tamaño en bytes de un elemento de referencia (archivo HTML, GIF, JPG, PDF, animación, etc.). El tamaño de un elemento incide directamente en el tiempo de descarga del mismo, entre más pesado sea el elemento (más bytes) mayor será el tiempo de descarga.

Portal: Sitio Web cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios, entre los que suelen encontrarse buscadores, foros, compra electrónica, por mencionar algunos. Principalmente están dirigidos a resolver necesidades específicas de una comunidad o dar acceso a la información y servicios de a una institución pública o privada.

Red: Es un conjunto de computadoras y/o dispositivos conectados por enlaces de un medio físico o inalámbricos y que comparten información (archivos), recursos (como lectores de CD-ROM o impresoras) y servicios (e-mail, Chat, juegos, entre otros).

Sharepoint: Plataforma de trabajo colaborativo y gestión documental especialmente orientada a documentos Microsoft Office.

Sitio Web: Punto de la red con una dirección única y al que pueden acceder los usuarios para obtener información. Normalmente un sitio Web dispone de un conjunto de páginas organizadas a partir de una página principal o "home page", e integra archivos de varios tipos, tales como sonidos, fotografías o aplicaciones interactivas de consulta (formularios). Sólo cuando un sitio tiene una sola página los términos de sitio y página son equivalentes.

Spam: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Usabilidad: Es la capacidad del sitio por medio de la cual el contenido Web puede ser comprendido, aprendido, usado y ser atractivo para el usuario, en condiciones específicas de uso.

www (World Wide Web): Literalmente es "telaraña mundial", mejor conocida como Web, compuesta de archivos de texto, multimedia y otros servicios (FTP, HTTP, telnet, Usenet, WAIS, etc.) conectados entre sí por medio de un sistema de documentos de hipertexto.
WSUS(Windows Server Update Services): Servidor que provee de actualizaciones de Seguridad para los sistemas operativos y productos Microsoft que realiza actualizaciones automáticas, según reglas configuradas según las necesidades del HUS.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

1. PRINCIPIOS DE SEGURIDAD

Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
Confidencialidad: La información sólo debe ser legible para los autorizados.
Disponibilidad: Debe estar disponible cuando se necesita.
Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

1.1. CONSEJOS BÁSICOS DE SEGURIDAD

Es recomendable seguir una serie de consejos, prácticas y costumbres para maximizar la seguridad informática en la E.S.E. Hospital Universitario de la Samaritana, algunos de ellos son los siguientes:

a) Mantener actualizado el equipo (Sistema Operativo y aplicaciones).
b) Hacer copias de seguridad con frecuencia.
c) Instalar software legal (se obtiene garantía y soporte).
d) Usar contraseñas fuertes (Evitar nombres, fechas, datos conocidos o deducibles, etc.).
e) Utilizar herramientas de seguridad para proteger o reparar el equipo.
f) No descargar o ejecutar ficheros desde sitios sospechosos o procedentes de correos desconocidos.
g) Analizar con el antivirus todo lo que se descargue.
h) No facilitar la cuenta de correo a desconocidos o publicarla en sitios desconocidos.
i) No responder a mensajes falsos.

1.2. REVISIONES PERIÓDICAS Y POR MUESTREO DEL SOFTWARE DEL HOSPITAL

El proceso de gestión de la información tiene la facultad de establecer revisiones periódicas y por muestreo de los software, aplicativos y programas que contienen los Computadores de escritorio y portátiles de la entidad usando cualquier mecanismo disponible en el hospital.

1.3. RESPONSABILIDAD LEGAL Y DISCIPLINARIA

En el caso de encontrarse software instalado en los equipos del hospital, que no cuenten con la debida autorización el proceso de gestión de la información podrá remitir de caso a se remitirá el caso a la oficina Asesora Jurídica quien lo tramitara dependiendo el tipo de vinculación laboral

2. SITIOS WEB DE LA ESE HOSPITAL UNIVERSITARIO DE LA SAMARITANA.

2.1. SITIOS WEB INSTITUCIONALES BAJO EL MISMO DOMINIO.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

Todos los Sitios Web Institucionales están bajo el dominio: hus.org.co.

2.2. CONTENIDO DE INFORMACIÓN Y SERVICIOS.

El Sitio Web Institucional contempla tanto el propósito de difusión la información relevante para la comunidad Hospitalaria y Universitaria, como el desarrollo de servicios y sistemas en línea que faciliten la información correcta y completa para la comunidad a la que atiende.

Los contenidos publicados mantienen el uso de un lenguaje simple y claro, especialmente en las páginas de difusión y servicios, que permite a los lectores concentrarse en el mensaje que recibe. Como complemento se ha revisado la estructura gramatical, el uso de palabras apropiadas, la ortografía y redacción de la información publicada.

El proceso del HUS que desee publicar información de importancia en el sitio Web deberá presentar el contenido en medio magnético, lo anterior no aplica a los procesos a los que previamente les fue asignada la administración de secciones específicas.

Debe contener:

a. Titulo completo y resumido (máximo 20 caracteres).
b. Tipo de publicación (noticia, información general, articulo, evento).
c. Resumen de no más de 10 renglones dentro de un documento en Microsoft Word (.doc) letra Times New Roman tamaño 12.
d. Debe evidenciarse la ubicación de los elementos insertados y párrafos en que se sugiere sea publicada la información posteriormente sujeta a las posibilidades que brinda el gestor de contenido.
e. De requerirse un elemento especial diferente a imágenes y texto tales como animaciones, botones, se debe suministrar junto con los archivos originales (fuentes).
f. El nombre de una persona, teléfono o correo electrónico que sirva como contacto que dé asesoría o canalice solicitudes, dudas o comentarios de los usuarios acerca del sitio y su contenido.

2.3. LINEAMIENTOS DE USO DE CADA SITIO.

Según sea el caso de cada sitio, se muestran los lineamientos de uso del mismo y/o confidencialidad de la información en él publicada, los términos y condiciones bajo los cuales se preste algún servicio, así como las exclusiones aplicables.

2.4. CONTENIDO GRÁFICO

Los sitios web institucionales contienen una identidad gráfica que transmite el sentido de pertenencia institucional a su comunidad, utilizan combinaciones de colores que identifiquen a la E.S.E. Hospital Universitario de la Samaritana.

a. Las imágenes no sustituyen el uso del Texto.
b. El uso de animaciones es limitado.
c. Las imágenes de ser posible están en formatos ligeros.

2.5. BÚSQUEDA DE INFORMACIÓN.

a. Los resultados de las búsquedas proveen información precisa respecto a la página que contiene las palabras clave.
b. Resalta las palabras clave en la lista de resultados y no proporciona listas de resultados muy extensas.
c. Las búsquedas tratan las mayúsculas, minúsculas y los acentos como caracteres equivalentes, por ejemplo: “mexico”, “MEXICO” y “México” y deben dar el mismo resultado.
d. Proporciona la opción de búsqueda en todas las páginas del sitio.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

e. Informar usuario de todos los tipos de búsqueda que proporciona el sitio para que él usuario seleccione el que mejor sirva a sus necesidades.

2.6. VERSIONES EN INGLÉS.

a. Las secciones más relevantes de todos los sitios Web en el hospital se presentan en idioma inglés.
b. Las unidades funcionales que deseen promover eventos o información en la página principal del Hospital, deberán hacer llegar la información en español y en inglés al Comité de Editorial y Comunicaciones.
c. Las traducciones al inglés serán responsabilidad de cada proceso y deberá ser realizada de manera profesional y libre de errores de redacción y ortografía.

2.7. ACCESO MÓVIL.

a) Las secciones más relevantes de todos los sitios Web en el Hospital contemplan versiones para dispositivos móviles, así como los mecanismos para su impresión.

2.8. NAVEGACIÓN

La navegación en la página WEB del Hospital y la Intranet y tiene las siguientes características:

a. Proporcionan un menú de navegación al inicio de la página. .
b. Mantiene el número de pulsaciones de teclas al mínimo.
c. Reduce la captura de texto, proporcionando valores por defecto preseleccionados.
d. Proporciona mensajes de error claros y mecanismos de navegación para regresar a la página anterior.

2.9. DISPONIBILIDAD.

El Sitio Web Institucional está disponible los 7 días de la semana y las 24 horas del día, incluyendo los periodos vacacionales y los fines de semana.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

3. MANEJO DEL CORREO ELECTRÓNICO INSTITUCIONAL.

3.1. LINEAMIENTOS GENERALES DE USO DE CORREO ELECTRÓNICO.

El correo electrónico institucional es una herramienta que la E.S.E. Hospital Universitario de la Samaritana proporciona a sus colaboradores para facilitar y optimizar el flujo de información de sus diferentes procesos y proyectos, por lo tanto es obligación de todos los funcionarios darle el mayor y correcto uso relacionado con sus labores diarias, evitando y disminuyendo al máximo el uso innecesario de papel.

3.2. SOLICITUD Y ASIGNACIÓN DE CUENTAS DE CORREO ELECTRÓNICO.

3.2.1. SOLICITUD DE CUENTAS

- Los únicos Funcionarios Autorizados para solicitar cuentas de correo electrónico son:
  a. El Gerente.
  b. Líderes de proceso, jefes Oficinas Asesoras, Directores, Subdirectores y Coordinadores de Unidades Funcionales.
- Es responsabilidad de cada líder de proceso autorizado (según la norma anterior):
  a. Definir cuáles de sus funcionarios requieren cuenta de correo electrónico, de acuerdo con sus funciones.
  b. Solicitar las cuentas de correo electrónico para cada uno de ellos, en el medio escrito establecido en el proceso actual.
- Cada líder de proceso, Jefe Oficina Asesora, Director, Subdirector y/o Coordinador de Unidad Funcional que requiera cuenta de correo electrónico para sí o para alguno de sus colaboradores deberá enviar la solicitud al Subdirector de Sistemas de la E.S.E. Hospital Universitario de la Samaritana, en el medio escrito establecido en el proceso actual.

3.2.2. CREACIÓN Y ASIGNACIÓN DE CUENTAS.

El único proceso de la E.S.E. Hospital Universitario de la Samaritana encargada de la creación y asignación de cuentas de correo electrónico a sus funcionarios es el proceso de gestión de la información. Dichas cuentas dispondrán de un Nombre de Usuario y una Contraseña, para permitir la identificación y el control de ingreso del funcionario a su cuenta asignada.

3.2.3. ASIGNACIÓN DE CUENTAS CON NOMBRES GENERICOS, PARA FUNCIONARIOS.

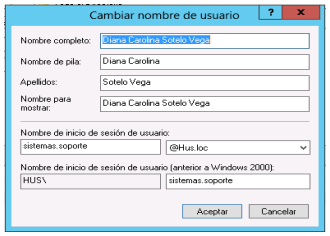
Las cuentas de correo electrónico para funcionarios de los procesos operativos en todos los servicios y procesos del Hospital, deberán asignarse con un Nombre de Usuario el cual es conformado por el nombre de área al que el trabajador va formar parte y el rol que va desempeñar en la misma.

<área><Punto ><rol>@hus.org.co

Ejemplo: Si se solicita cuenta de correo electrónico para un funcionario cuyo nombre completo es Diana Carolina Sotelo Vega que realizara labores en el área de sistemas, desempeñándose en el rol de soporte técnico dicha cuenta deberá ser asignada con el siguiente nombre de usuario:

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

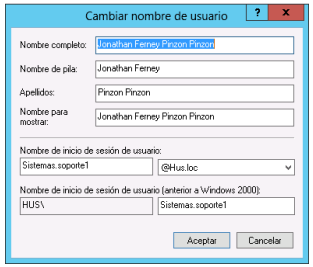
sistemas.soporte@hus.org.co



3.2.4. REPETICIÓN DE ROL.

Si en el momento de asignación de un nombre de usuario se detecta que ya se encuentra una persona ejerciendo el Rol, se incluirá para el nuevo nombre de usuario un numero consecutivo iniciando por el numero1, al final del Rol por ejemplo, Si se solicita cuenta de correo electrónico para un funcionario cuyo nombre completo es Jonathan Ferney Pinzón Pinzón que realizara labores en el área de sistemas, desempeñándose en el rol de soporte técnico dicha cuenta deberá ser asignada con el siguiente nombre de usuario:

sistemas.soporte1@hus.org.co



De igual Forma si ingresa más personal que asumen el mismo Rol se incluirán los números consecutivos según sean pertinentes.

3.2.5. DEFINICIÓN DE CONTRASEÑAS.

En el momento de la creación y asignación de la cuenta, se le pedirá al usuario que defina su contraseña la cual debe cumplir con las siguientes características:

a. No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
b. Tener una longitud mínima de ocho caracteres
c. Incluir caracteres de tres de las siguientes categorías:

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

d. Mayúsculas (de la A a la Z)
e. Minúsculas (de la A a la z)
f. Dígitos de base 10 (del 0 al 9)
g. Caracteres no alfanuméricos (por ejemplo ! $, #, %)
h. Constituido por caracteres alfanuméricos de la A a la Z y del número 1 a 9.
i. Es recomendable no ser un nombre de obvio reconocimiento o predicable.
j. La contraseña Caduca cada 90 días y pedirá cambio.
k. No está permitido el uso de las tres últimas contraseñas utilizadas.

En los casos en que el funcionario olvide su contraseña o sospeche sobre el uso fraudulento de su cuenta, debe dirigirse al líder de proceso, Jefe Oficina Asesora, Director, Subdirector y/o Coordinador de Unidad Funcional.

El usuario puede cambiar la contraseña desde un computador con la opción de Windows al oprimir simultáneamente Ctrl+Alt+Supr y seleccionando cambiar contraseña, cabe resaltar que esta contraseña, es la misma que se utiliza en correo, mesa de ayuda ya que estos sistemas realizan autenticación sobre el directorio activo. Los usuarios de directorio activo son los mismos de correo.

3.2.6. ACTUALIZACIÓN DE CUENTAS.

Cada líder de proceso, Director, Subdirector y/o Coordinador de Unidad Funcional debe registrar y administrar y la información de los funcionarios a su cargo que sean usuarios del correo electrónico institucional (incluyéndose el mismo), así como "actualizar", reportar los cambios que se produzcan en dicha información (vacaciones, licencias, retiro, traslado); se debe suministrar la información oportunamente a la Proceso de Gestión de la Información a más tardar al día hábil siguiente del conocimiento de la novedad quienes procederán a:

a. Inactivar las cuentas de correo electrónico correspondientes.
b. Asignar dichas cuentas a usuarios cuya solicitud de este servicio este en trámite.

3.3. NORMAS GENERALES SOBRE EL USO DEL CORREO ELECTRÓNICO INSTITUCIONAL.

3.3.1. DERECHOS DE LOS USUARIOS DEL CORREO ELECTRÓNICO.

a. Todos los usuarios tienen derecho a la privacidad de sus mensajes de correo electrónico, cuando se usa como herramienta de trabajo para sus labores.
b. Todo usuario tiene derecho a recibir atención por parte de la Proceso de Gestión de la Información y obtener soluciones rápidas y oportunas a inconvenientes relacionados con el servicio de correo electrónico, siempre y cuando se reporte con anterioridad.
c. Si un usuario se siente ofendido por el contenido de un mensaje tiene derecho a expresar su inconformidad**,** reenviar el mensaje a la cuenta del Cargo de Subdirector de Sistemas, quien atenderá y tomará las acciones correctivas pertinentes, incluyendo Comité de Convivencia Conciliaciones o a la Oficina de Control Disciplinario.

3.3.2. RESPONSABILIDADES GENERALES DE LOS USUARIOS DE CORREO ELECTRÓNICO.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

a. No emplear el correo electrónico institucional en contra de los intereses de personas individuales, ni de la de ninguna otra institución.
b. Mantener siempre abierto el programa de correo electrónico desde el inicio de la jornada laboral y siempre que esté trabajando en su computador.
c. Consultar y leer diariamente el correo electrónico y responder oportunamente a las solicitudes de los mensajes.
d. Mantener en orden cada una de las carpetas que conforman su buzón de correo y eliminar los mensajes innecesarios.
e. Abstenerse de leer correos cuyo remitente no conozca.
f. No enviar mensajes a destinatarios desconocidos, sin razón laboral de por medio, a menos que exista justificación suficiente.
g. Revisar siempre que el envío de los mensajes se realice a los destinatarios correctos.
h. Todo usuario de correo será responsable de los perjuicios que ocasione a su proceso por la pérdida de confidencialidad causada por información enviada a un destinatario incorrecto.
i. Generar mensualmente copias de seguridad de la Totalidad de la información existente en sus carpetas personales de correo electrónico, siguiendo el procedimiento indicado en el "***instructivo",*** Manual de Back Up correspondiente.
j. Realizar y administrar un archivo propio con todos los documentos e información recibida por el correo electrónico institucional de instancias superiores a la E.S.E. Hospital Universitario de la Samaritana (tales como la Junta Directiva del Hospital, Ministerio de Protección, Superintendencia Nacional de Salud, ASEMI, etc.).
k. En general, todo usuario de correo electrónico institucional es responsable del conocimiento y estricto cumplimiento de las lineamientos, normas, procedimientos y estándares de seguridad definidas por la Gerencia y la Proceso de Gestión de la Información, específicamente las establecidas en el presente manual.
l. El manejo de las direcciones de correo electrónico genéricas asignadas a cada departamento o dependencia son responsabilidad del líder de proceso, Director, Subdirector y/o Coordinador de Unidad Funcional y podrán delegar la atención de dicha cuenta de correo, sin eximirse de la responsabilidad por el cumplimiento de las presentes normas e independientemente del accionar del personal en el cual delegue tales funciones.

3.3.3. USO PERSONAL E INTRANSFERIBLE.

a. Cada nombre de usuario y contraseña asignados a un funcionario para el uso de su cuenta serán de carácter personal e intransferible y no podrán divulgarse, en caso de hacerlo, el funcionario responderá administrativa y judicialmente por actos fraudulentos.
b. El correo electrónico institucional es de carácter laboral y su uso es exclusivo para ese tipo
c. El usuario debe evitar omisiones de su parte que faciliten el acceso a su cuenta, tales como:

Definir contraseñas con nombre y usuario iguales.
Escribir la contraseña en sitios visibles excepto para cuentas genéricas de servicios que rotan personal.
Dejar escrita la clave en documentos electrónicos en la red
Dejar su computador encendido con una sesión abierta de correo
Guardar automáticamente las contraseñas

3.3.4. ÚNICO PROGRAMA PARA ENVÍO DE CORREO ELECTRÓNICO.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

El personal de la E.S.E. Hospital Universitario de la Samaritana solo está autorizado a utilizar el correo electrónico institucional como herramienta de trabajo para sus labores, ya que la Proceso de Gestión de la Información no puede realizar copias de seguridad correos diferentes al institucional..

3.3.5. TIPOS DE USO AUTORIZADO PARA EL CORREO ELECTRÓNICO.

Todos los funcionarios con cuenta de correo electrónico institucional podrán utilizarla para los siguientes propósitos:

a. Comunicación e Intercambio de información entre las dependencias y los funcionarios del Hospital.
b. Comunicación entre entidades gubernamentales y estatales que tengan relación con la labor desempeñada.
c. Comunicación con investigadores, economistas y personas relacionadas con las labores desempeñadas en la Institución, en el ámbito nacional y extranjero.
d. Comunicación e intercambio de información con la comunidad académica, universitaria u otras instituciones con el fin de tener acceso a los últimos avances relacionados con el negocio de la y que contribuyan a la misión de la Institución y de su proceso.
e. Cualquier otro que se considere conveniente para la ejecución de las labores encomendadas y el beneficio de la institución.

3.3.6. USO NO AUTORIZADO DEL CORREO ELECTRÓNICO.

El correo electrónico es de uso exclusivamente para uso laboral, por lo tanto queda prohibido:

a. Envío de cadenas de mensajes conocidas como Spam o Hoax (engaños masivos por medios electrónicos).
b. Envío de archivos ejecutables como protectores de pantalla y animaciones, ya que pueden contener virus informáticos nocivos.
c. Utilizar el correo para insultar, intimidar, acosar o interferir en el trabajo de los demás.
d. Provocar el mal funcionamiento de computadores, estaciones o terminales periféricos de redes y sistemas.
e. Poner información que infrinja los derechos de los demás.
f. Utilizar el correo para fines lucrativos o comerciales.
g. Comunicación e información con lugares obscenos que perjudiquen u ofendan a terceros, asimismo el recibir mensajes con contenido obsceno que no tenga relación con su desempeño laboral.
h. Enviar información confidencial a usuarios que no pertenecen a la institución o que no esté autorizada a recibirla.
i. Cualquier otro que se considere perjuicio para la institución.

3.3.7. NORMAS GENERALES PARA LA REDACCIÓN Y ENVÍO DE MENSAJES DE CORREO ELECTRÓNICO.

a. Se debe emplear una redacción y presentación apropiada de los mensajes empleando correctamente los signos de puntuación para que el mensaje no sea mal interpretado.
b. NO USAR LETRAS MAYÚSCULAS EN LA REDACCIÓN DE MENSAJES DE CORREO ELECTRÓNICO ya que da la impresión de “grito” tal como se aprecia en la oración anterior.
c. Abstenerse de incluir imágenes, iconos, papel tapiz o fondo diferente al establecido por el Proceso de Gestión de la Información, pues va en contra de la imagen institucional de la E.S.E. Hospital Universitario de la Samaritana, además de ocasionar lentitud en el envío de mensajes.
d. Debe digitar siempre el nombre o motivo del mensaje en el campo”Asunto”, y debe definirse resumidamente el asunto del mensaje de la forma más clara y concisa.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

e. Cuando reenvíe un mensaje conserve en él su mensaje original, para que los destinatarios puedan conocer el motivo original o inicial del mensaje reenviado.

3.3.8. ENVÍO Y MANEJO DE LAS COPIAS.

Solo se puede enviar copias de un determinado mensaje a destinatarios para quienes sea absolutamente indispensable:

a. Ejecución de sus labores diarias.
b. Participación y comunicación en determinado proyecto a los directos involucrados.
c. Confirmación de resultados o tareas encomendadas.
d. Capacitación, normalización o información de interés general para el Hospital.

El cumplimiento de esta norma evitará sobrecarga del servidor de correo electrónico que afecta negativamente la velocidad de respuesta y su capacidad de almacenamiento, los únicos funcionarios autorizados para enviar copias de sus mensajes a la Gerencia son los directivos que dependen directamente de ella. Los demás funcionarios sólo podrán hacerlo con autorización expresa de sus jefes inmediatos o por solicitud directa de la Gerencia.

3.3.9. DESACTIVACIÓN Y ACTIVACIÓN DE LAS CUENTAS DE CORREO ELECTRÓNICO.

3.3.9.1. DESACTIVACIÓN.

Una cuenta de correo electrónico institucional será desactivada por la Proceso de Gestión de la Información por las siguientes razones:

a. No ingresar a la cuenta de correo por un periodo igual o mayor a treinta (30) días calendario.
b. Solicitud del Jefe inmediato del funcionario usuario.
c. Uso indebido del correo electrónico o incumplimiento de sus normas.
d. Novedades de personal: Retiros, traslados, ingresos, vacaciones, licencias, viajes laborales o cambios de cargo o función.

3.3.9.2. ACTIVACIÓN.

En el evento de desactivación de la cuenta de correo electrónico por cualquiera de las razones anteriores, el jefe inmediato del funcionario afectado deberá solicitar la activación mediante solicitud escrita dirigida al Proceso de Gestión de la Información en la que explique o justifique la razón de la inactivación y la necesidad de la nueva activación.

3.3.10. IMPRESIÓN DE MENSAJES.

No se deben imprimir ni archivar los mensajes de correo electrónico de tipo informal (Se considera correspondencia informal la originada entre usuarios en eventos casuales como: recordar reuniones, solicitar conceptos, invitaciones).

3.3.11. ADICIÓN DE ARCHIVOS A LOS MENSAJES DE CORREO ELECTRÓNICO.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

a. Los únicos archivos que los funcionarios de la E.S.E. Hospital Universitario de la Samaritana podrán adjuntar a sus mensajes de correo electrónico serán aquellos generados por los programas y aplicativos debidamente autorizados e instalados en sus computadores por la Proceso de Gestión de la Información.
b. El tamaño límite para el envío de archivos adjuntos a los mensajes del correo electrónico institucional es de diez Veinte Megabytes (20 Mb) por mensaje, es decir que la suma del tamaño de los archivos a adjuntar a un mensaje no debe superar los 20 Mb Esto con el fin de evitar la saturación de los canales de comunicación (entre el emisor y el receptor).

Cuando deba enviar por correo electrónico un archivo que supere el máximo tamaño permitido, deberá procederse de la siguiente forma:

a. Comprimir el archivo mediante el programa de compresión proporcionado por la E.S.E. Hospital Universitario de la Samaritana.
b. Si después de la compresión del archivo este todavía supera el tamaño máximo permitido, deberá fraccionar el archivo original (no comprimido) en archivos más pequeños que no superen cada uno el tamaño máximo permitido.
c. Si aun así los archivos obtenidos superan cada uno el tamaño máximo permitido, el funcionario usuario deberá solicitar apoyo a Soporte Técnico, mediante comunicación telefónica a la Ext. 10104 o 10105.
d. Por seguridad los archivos adjuntos con las siguientes extensiones no serán aceptados (*.ad,*.ade,*.adp,*.asp,*.bas,*.bat,*.chm,*.cmd,*.com,*.cpl,*.crt,*.exe,*.hlp,*.hta,*.inf,*.ins,*.isp,*.js,*.jse,*.lnk,*.mdb,*.mde,*.msc,*.msi,*.msp,*.mst,*.pcd,*.pif,*.reg,*.scr,*.sct,*.shb,*.shs,*.url,*.vb,*.vbe,*.vbs,*.vsd,*.vss,*.vst,*.vsw,*.ws,*.wsc,*.wsf,*.wsh.)
e. Por seguridad los archivos adjuntos encriptados o con clave en correos entrantes no serán admitidos.

3.3.12. NOTIFICACIÓN DE FALLAS, INCONSISTENCIAS Y ANOMALÍAS.

Todo funcionario de la E.S.E. Hospital Universitario de la Samaritana deberá notificar a Soporte Técnico sobre cualquier falla, anomalía, inconsistencia, incidente o violación de seguridad que descubra, relacionada con el servicio de correo electrónico Institucional, mediante cualquiera de las siguientes vías:

a. Mensaje de correo electrónico a la cuenta del Cargo de Subdirector de Sistemas
b. Comunicación telefónica las Ext. 10104 o 10105.

NOTA: La oportuna y rápida respuesta a los requerimientos de Soporte Técnico respecto al servicio de correo electrónico depende igualmente de la rapidez y celeridad con que el funcionario reporte estas situaciones a Soporte Técnico.

3.4. DIVULGACIÓN Y DISTRIBUCIÓN MASIVA DE CORREO Y ARCHIVO SOBRE NORMATIVIDAD E INFORMACIÓN GENERAL.

a. La funcionalidad de entrada y salida de mensajes del correo electrónico institucional desde y hacia Internet sólo debe usarse con fines laborales.
b. Las únicas dependencias de la E.S.E. Hospital Universitario de la Samaritana autorizadas para clasificar y controlar el correo que debe salir y entrar a la empresa son:

Gerencia.
Oficinas Asesoras.
Direcciones.
Subdirecciones.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

Comunicaciones.

c. Todo documento de carácter normativo o informativo (distinto a memorando) que requiera ser enviado a través del correo electrónico Institucional, deberá anexarse a los mensajes de correo, en forma de documentos adjuntos, utilizando los formatos autorizados por la Gerencia para tal fin.

d. Los mensajes masivos para personal interno deben ser filtrados a través del área de Comunicaciones esta oficina es la encargada del envió de los mismos.

3.5. SEGURIDAD, ENVÍO Y RECEPCIÓN DE INFORMACIÓN DE TRABAJO DESDE Y HACIA FUERA DEL HOSPITAL.

a. La funcionalidad de entrada y salida de mensajes del correo electrónico institucional desde y hacia Internet solo debe usarse con fines laborales

b. Las únicas dependencias de la E.S.E. Hospital Universitario de la Samaritana autorizadas para clasificar y controlar el correo que debe salir y entrar a la empresa son:

Gerencia.
Oficinas Asesoras.
Direcciones.
Subdirecciones.

c. No se debe incluir la dirección de correo electrónico institucional en suscripciones personales de Internet con "Lista de amigos" pues esto provoca que gran cantidad de mensajes externos lleguen a su casilla de correo provocando saturación de los canales de comunicación.

3.6. NORMAS DE SEGURIDAD CONTRA VIRUS INFORMÁTICOS.

3.6.1. ÚNICO PROCESO AUTORIZADO PARA DISTRIBUIR EL ANTIVIRUS.

Las únicas cuentas de correo electrónico habilitadas para advertir a los usuarios sobre el riesgo de virus informáticos y de proporcionarles los programas antivirus y los archivos relacionados con la protección ante dicho riesgo son las que pertenecen a los funcionarios de Soporte Técnico del proceso de gestión de la información.

3.6.2. REMITENTES SOSPECHOSOS.

No se deben abrir mensajes de correo electrónico con remitentes con estas características:

a. De remitente desconocido y cuya cuenta no pertenezca a la Institución o provenga de Internet.
b. Cuyo asunto esté en idioma diferente al español.
c. Que prevengan sobre posibles virus, ofrezcan algún producto, servicio o distracción o alerten sobre cualquier tipo de riesgo o amenaza.
d. Que provengan de cuentas de correo con el dominio de la E.S.E. Hospital Universitario de la Samaritana pero con nombre desconocido (Ejemplo: comiteelectoral@hus.org.co, admin@hus.org.co; antivirus@hus.org.co, john@hus.org.co.).

3.6.3. PARA EVITAR LA APERTURA ACCIDENTAL DE LOS MENSAJES ENUNCIADOS EN LA FORMA ANTERIOR SE DEBE:

a. Deshabilitar el "Panel de Vista Previa" y la opción de "Vista Previa Automática", en el menú "Ver" de su programa de correo electrónico.
b. NO debe tenerse habilitada la función de Outlook: "Mostrar un aviso de notificación cada vez que llega un correo". En caso de que aún no haya deshabilitado esta función y

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

aparezca en su pantalla el mensaje correspondiente preguntándole si desea leerlo ahora, seleccione la opción "NO", y consulte luego su bandeja de entrada para verificar el remitente y su asunto, con la debida precaución y cautela.

3.6.4. ELIMINACIÓN DE ARCHIVOS CONTAMINADOS NO LIMPIADOS.

Cada vez que el programa antivirus del computador del funcionario usuario detecte la existencia de un mensaje de correo o archivo contaminado con virus y no pueda limpiarlo, avisará sobre esta situación al usuario, advirtiéndole sobre el peligro de abrir o ejecutar dicho archivo. El usuario, en este caso tiene la obligación de eliminar este archivo tanto de su bandeja de entrada de correo electrónico como del disco duro de su computador.
Adicionalmente, deberá Informar de esta situación al proceso de gestión de la información de la E.S.E. Hospital Universitario de la Samaritana.
El funcionario será responsable de los daños ocasionados a la información y equipos de cómputo de propiedad de la E.S.E. Hospital Universitario de la Samaritana, derivados del incumplimiento de esta norma.

3.6.5. RESERVA DE PROPIEDAD DE LAS SOLUCIONES ANTIVIRUS.

Los mensajes de advertencias contra virus y sus archivos de actualización y programas anexos, proporcionados por la Proceso de Gestión de la Información, son confidenciales y propiedad de la E.S.E. Hospital Universitario de la Samaritana y para uso exclusivo de la persona o entidad de destino.
Queda terminantemente prohibida la copia, reimpresión o reenvió del mismo por parte del usuario de la cuenta de correo.
En caso de que un funcionario del Hospital reciba uno de estos mensajes y/o archivos por error u omisión deberá notificar inmediatamente el evento al Cargo de Subdirector de sistemas del Hospital (Dirección de correo: subdirector.sistemas@hus.org.co).

3.7. NORMAS ESPECÍFICAS DE SEGURIDAD Y ADMINISTRACIÓN DE LA PROCESO DE GESTIÓN DE LA INFORMACIÓN.

3.7.1. ADMINISTRACIÓN DEL SERVICIO.

La Proceso de Gestión de la Información se reservará el derecho de verificar el contenido de los mensajes de correo electrónico generados por los usuarios en los casos en que medie una solicitud expresa de autoridades competentes, para los fines que se estimen convenientes.
El Proceso de Gestión de la Información tiene la autoridad y responsabilidad de controlar y negar el acceso al correo electrónico institucional a cualquier funcionario del Hospital que infrinja sus normas y lineamientos establecidos o que interfiera con los derechos de otros usuarios de correo electrónico.
Adicionalmente, la Proceso de Gestión de la Información, a través de Soporte Técnico, deberá:

a. Garantizar el normal funcionamiento del servicio de correo electrónico institucional, así como atender los requerimientos y solucionar oportunamente los inconvenientes de los usuarios del servicio.
b. Establecer e implementar mecanismos que garanticen la confidencialidad de la información trasmitida a través del correo electrónico.
c. Establecer y divulgar mecanismos que permitan a los usuarios del servicio de correo electrónico realizar copias de respaldo de sus mensajes, cuando sea necesario, así como de proveer e informar sobre el medio de almacenamiento de estas copias (Consultar el documento: "Procedimiento para la Generación de Backups de Archivos de Trabajo", expedido por la Gerencia).
d. Ejecutar la creación y eliminación de las cuentas de correo electrónico, según las solicitudes de los líderes de proceso.
e. Garantizar a cada funcionario, a quien se le asigne cuenta de correo electrónico, el cumplimiento de los requisitos mínimos de hardware y de software para la instalación y correcto funcionamiento de su cuenta de correo.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

3.7.2. Intercambio Electrónico de Datos

Él Hospital puede realizar convenios y/o contratos para el manejo de algún tipo específico de información, para la realización de estas actividades de intercambio electrónico de datos, la proceso de Gestión de la Información realizara un envío de información, el proveedor realizar las actividades necesarias para su procesamiento, para que la información procesada será retornada al área específica del hospital a través de los medios que el proceso de gestión de la información provea.

3.7.3. FIRMA AUTOMÁTICA Y RESERVA DE PROPIEDAD DE LA INFORMACIÓN.

Será función y responsabilidad de la Proceso de Gestión de la Información insertar la firma institucional del funcionario en el momento de la instalación de cuenta en su computador, con las siguientes características:

a. Que aparezca al final de todo mensaje a enviar.
b. Incluirá el nombre completo (Nombre y Apellidos) del funcionario usuario dueño de la cuenta
c. Después del nombre ira el cargo dentro de la organización.
d. Nombre del área al que funcionario hace parte. Seguido el correo y por ultimo teléfono y extensión.
e. Al final de la firma deberá aparecer el siguiente mensaje o norma para aplicación y cumplimiento de la totalidad de los funcionarios del hospital:

"La información transmitida a través del correo electrónico institucional es confidencial y está dirigida únicamente a su destinatario. Su reproducción, lectura o uso está prohibido a cualquier persona o entidad diferente.

La E.S.E. Hospital Universitario de la Samaritana no se hace responsable por la eventual transmisión de virus o programas dañinos por este conducto.

Las opiniones, conclusiones y otra información contenida en los mensajes de correo no relacionados con el negocio oficial dela E.S.E. Hospital Universitario de la Samaritana, se entienden como personales y de ninguna manera serán avalados por la E.S.E. Hospital Universitario de la Samaritana".

3.7.4. TIEMPO DE RESPUESTA PARA LAS SOLICITUDES.

Para los siguientes tipos de solicitud de correo electrónico, el tiempo de trámite por parte de Soporte Técnico es como máximo de un (1) día hábil (contado a partir de la recepción de dicha solicitud):

a. Creación de Cuentas para usuario temporal.
b. Creación de Cuentas para usuario definitivo.
c. Bloqueo de cuenta por vacaciones, licencias, viajes laborales o por seguridad (cuando se sospecha de la pérdida de confidencialidad de la contraseña).
d. Activación de cuentas.
e. Cancelación de cuentas por desvinculación laboral.
f. Cambio de cuenta por traslado entre áreas o ascensos.
g. Solicitud de nueva contraseña.

3.7.5. CONFIGURACIÓN DE FECHA Y HORA CORRECTA.

El Proceso de Gestión de la Información garantizará que los computadores personales de los funcionarios usuarios de correo electrónico se encuentren siempre configurados con la fecha y hora correcta. El cumplimiento de esta norma redundará en la veracidad y claridad de toda la información enviada a través del correo electrónico institucional.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

3.7.6. NORMAS ESPECÍFICAS DE SEGURIDAD.

a. La Proceso de Gestión de la Información, mediante Soporte Técnico, deberá garantizar la confidencialidad y discreción de la información que repose en los mensajes.
b. La Proceso de Gestión de la Información efectúa el proceso de Backup (generación de copia de respaldo) al correo institucional.

3.7.7. PROCEDIMIENTOS.

3.7.7.1. SOLICITUD, TRÁMITE E INSTALACIÓN DE UNA CUENTA DE CORREO.

DESCRIPCIÓN GENERAL.

Este procedimiento describe la solicitud, asignación e instalación de una cuenta de correo electrónico, para cualquier funcionario de HOSPITAL UNIVERSITARIO DE LA SAMARITANA que la requiera.

3.7.7.2. SOLICITUD Y APROBACIÓN INICIAL.

FUNCIONARIO SOLICITANTE – LÍDER DE PROCESO

a. Identifica las necesidades de correo electrónico de su área y determina cuál o cuáles de sus colaboradores requieren de asignación de cuenta de correo electrónico.
b. Envía la solicitud (o solicitudes) a la Proceso de Gestión de la Información del Hospital.

PERSONAL DE SISTEMAS.

a. Recibe la solicitud y genera el registro en la mesa de ayuda.
b. Se envía un mensaje de correo electrónico a cada solicitante, informándole el número asignado a su solicitud y su tiempo de respuesta (Mensaje automático).
c. Si la solicitud es actualmente viable, se comunica con el funcionario solicitante y le informa la aprobación de la cuenta.

3.7.8. ADMINISTRADOR DE CORREO ELECTRÓNICO.

Recibe la solicitud y crea la cuenta en el servidor de correo electrónico de la E.S.E. Hospital Universitario de la Samaritana.

PROCESO DE GESTIÓN DE LA INFORMACIÓN.

a. Le informa al funcionario que su cuenta se encuentra completamente creada y habilitada para ser usada, y continúa con el proceso.
b. Prueba la correcta creación de la cuenta y configuración respectiva solicitándole al funcionario usuario la prueba del mismo.

FUNCIONARIO USUARIO.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

a. Ingresa al correo y se envía un mensaje a su misma cuenta de correo electrónico (la que le acaban de configurar e instalar) y a la del Cargo del funcionario del proceso de gestión de la información que se encuentra atendiéndolo.
b. Confirma la correcta recepción de su mensaje en la Bandeja de Entrada de su cuenta.
c. Si recibió correctamente su mensaje, manifiesta su satisfacción, en acuse de recibido.

NOTA: La recepción efectiva del mensaje en el buzón del funcionario del área de sistemas, también sirve como registro y confirmación del correcto funcionamiento de la cuenta de correo electrónico instalada.

3.8. INSTRUCTIVO PARA LA REALIZACIÓN DE COPIAS DE RESPALDO DE LA INFORMACIÓN DEL CORREO ELECTRÓNICO.

OBJETIVO:

Indicar la forma correcta de realizar copias de seguridad al correo electrónico personal y de esta forma minimizar la perdida de información de los usuarios del correo electrónico ocasionada por daños en el computador o en el sistema operativo

4. GENERACIÓN DEL ARCHIVO DE BACKUP DE CORREO ELECTRÓNICO.

Ver manual de Backups sección Backups de correo electrónico.

5. PLAN DE CONTINGENCIA.

Ver plan de contingencia código.

6. RESPALDO ELÉCTRICO.

Se cuenta con una dos UPS. La cual soporta los equipos servidores y de comunicaciones del centro de cómputo. En el momento en que falla el fluido eléctrico se da aviso al dominio para que todos los funcionarios procedan a salvar sus trabajos y a apagar los computadores evitando así la perdida de información y daño en los equipos.
El servidor de Bases de Datos cuenta con su propia UPS.
Se cuenta además con una planta eléctrica la cual soporta las interrupciones del fluido eléctrico por un rango de tiempo más amplio, (para más detalles ver plan de contingencia)

7. LINEAMIENTOS PARA LLAMADAS A CELULAR.

7.1. CONTROL DE ACCESO PARA LLAMADAS A CELULAR.

a. El hospital cuenta con planes para llamadas a celular, disponibles durante el mes.
b. Para realizar una llamada a celular y/o larga distancia, se debe solicitar el código al Proceso de Gestión de la Información, previo visto bueno del director Administrativo.
c. En el momento en que se terminen de utilizar los minutos disponibles del mes, el hospital no contará con minutos y saldrá un mensaje informativo de la empresa de telefonía

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

celular.

7.2. USO DE LLAMADAS A CELULAR Y LARGA DISTANCIA.

a. Se puede realizar las llamadas desde las extensiones previamente configuradas según las necesidades del servicio.
b. Para llamadas a celular debe marcar primero el número 9 para sacar el llamada, el 03 para realizar llamadas a celular, el número de celular y el código asignado.
c. La vigencia del código estará determinada por el tiempo de vinculación del usuario con el hospital, para lo cual cada proceso deberá reportar a la Proceso de Gestión de la Información la desvinculación, para que su cuenta sea deshabilitada o eliminada, según la Proceso de Gestión de la Información estime necesario o por solicitud escrita del jefe inmediato, Director o líder de proceso correspondiente.
d. Las llamadas a celular y larga distancia, son para actividades de la institución y no para uso personal.

7.3. SEGURIDAD EN LA UTILIZACIÓN DE LLAMADAS A CELULAR Y LARGA DISTANCIA.

a. Al momento de marcar no dejar ver su clave.
b. Si cree que alguien conoce su código, puede solicitar el cambio en la Proceso de Gestión de la Información.

7.4. RESPONSABILIDADES EN EL USO DE LLAMADAS A CELULAR Y LARGA DISTANCIA.

a. La clave es personal e intransferible.
b. todas las llamadas realizadas desde este es responsabilidad del funcionario a quien se le asigna el código.
c. El mal uso de la clave, puede acarrear consecuencias tales como la cancelación temporal o permanente de la cuenta.
d. Cada uno de los usuarios es responsable del cumplimiento de los lineamientos y el líder de proceso deberá supervisar el cumplimiento de las mismas.

8. DIRECTRICES GENERALES DE SEGURIDAD INFORMÁTICA.

8.1. EQUIPO.

8.1.1. Instalación del equipo de cómputo.

a. Todo el equipo de cómputo (computadores, computadores portátiles, y otros accesorios), que esté o sea conectado a la red de datos del hospital o aquel que en forma autónoma se tenga debe sujetarse a las normas y procedimientos de instalación que emite la Proceso de Gestión de la Información.
b. La Proceso de Gestión de la Información en coordinación con Apoyo Administrativo debe tener un registro de todos los equipo propiedad del hospital.
c. El equipo de la institución que sea de propósito específico, requiere estar ubicado en un área que cumpla los requerimientos que la Proceso de Gestión de la Información tiene establecido en sus normatividad como: seguridad física, condiciones ambientales, alimentación eléctrica y control de acceso.
d. Los responsables de las distintas áreas de los departamentos deberán en conjunto con el Proceso de Gestión de la Información dar cumplimiento de las normas de instalación y notificaciones correspondientes de actualización, reubicación y todo aquello que implique cambios.
e. La protección física de los equipos corresponde a quienes se les asigna, además de notificar los movimientos que se hagan al Proceso de Gestión de la Información.
a. Los equipos que sean traídos por personal interno o externo al Hospital y que requiera ser incluidos en la red del hospital, o que se requiera acceso a internet, deben certificar de la legalidad de software instalado en la máquina, además el usuario que traiga el equipo será responsable de registrarlo ante la empresa de seguridad del

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

hospital, de su uso y de su seguridad física.

8.1.2. ASIGNACIÓN DEL EQUIPO DE CÓMPUTO.

b. Todo usuario del HUS al que se le asigne un equipo de cómputo (computadores, computadores portátiles, y otros accesorios) propiedad del HUS será responsable de su uso y de su seguridad física.
c. El usuario al que se le entrega el equipo de cómputo deberá firmar un acta de entrega donde se puntualizará el estado actual del equipo de cómputo en materia de hardware y software, y quedara registrado en la hoja de vida del equipo de cómputo.
d. El usuario debe verificar que el equipo de cómputo entregado cuente con todas las herramientas y configuraciones necesarias para su labor (Sistema de información, Antivirus, Procesador de texto, entre otros.)
e. En las áreas donde se tengan equipos de cómputo de propósito general tales como Biblioteca, Salas de capacitación, donde no se tenga identificado claramente el responsable de cada equipo, el líder de proceso deberá asignar una persona que asuma la responsabilidad sobre el uso que se le dé a esos equipos.

8.2. RESPONSABILIDADES Y CUIDADO DEL EQUIPO DE CÓMPUTO.

a. Los usuarios no deben intentar abrir los equipos de cómputos, impresoras, reguladores de voltaje, etc., ni manipular ninguna de sus partes.
b. Se prohíbe el consumo de alimentos cerca de los equipos de cómputo.
c. No deben ubicarse elementos como plantas, bebidas, sobre los equipos de cómputo y se debe evitar bloquear las rejillas de ventilación.
d. Cada usuario debe apagar su equipo de cómputo al finalizar la jornada de trabajo. , salvo los equipos que se requiere que estén prendidos las 24 horas.
e. El usuario es el encargado de asegurarse que su información este salvaguardada haciendo que sus archivos cuente con las protección necesarias de lectura, escritura y ejecución.
f. Es responsabilidad del usuario realizar el respaldo (copias de seguridad) de su información.
g. Si el usuario nota un mal funcionamiento del sistema, constantes mensajes de error, debe notificar la solicitud de la revisión a la Proceso de Gestión de la Información.
h. Todos los equipos de cómputo deben contar con un software antivirus instalado, activo y actualizado con la última versión del software, la administración del antivirus será centralizada y actualizada desde un equipo servidor.
i. Es responsabilidad del usuario realizar periódicamente revisiones antivirus en su equipo de cómputo. Los archivos en dispositivos USB, CD y DVD también pueden contener virus, por lo cual los usuarios deberán explorar los medios con el antivirus antes de intentar copiar o abrir los archivos que contengan; estos medios nunca deberán usarse para intentar iniciar el sistema.
j. La Proceso de Gestión de la Información se reserva el derecho de bloquear el acceso a las unidades/medios extraíbles con el fin de evitar la propagación de virus o para impedir la generación de vacíos de seguridad, que permiten la copia no autorizada de información de uso exclusivo del hospital.
k. Los usuarios no deben guardar archivos de tipo música, videos, fotografías, juegos, que no sean previamente autorizados o que hagan parte de la labor realizada por los funcionarios. Si en revisiones de software realizadas, se llegase a encontrar este tipo de archivos, el proceso de Gestión de la Información procederá a su eliminación sin la necesidad de dar un previo aviso.

8.3. CAMBIOS AL HARDWARE Y SOFTWARE.

a. Los equipos de cómputo no deben ser alterados (cambio de procesador, adición/retiro de tarjetas) sin el consentimiento y evaluación de la Proceso de Gestión de la Información.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

b. La actualización y cambios de hardware será llevada a cabo por la Proceso de Gestión de la Información, este proceso quedara registrado en la hoja de vida del equipo de cómputo, el usuario que tiene asignado ese equipo deberá firmar una nueva acta de entrega donde aparecerán los cambios.
c. Todos los equipos de cómputo del hospital están relacionados en un inventario donde aparecen las características, configuración y ubicación del mismo. La Proceso de Gestión de la Información es la encargada de controlar cualquier cambio y ejecución.
d. Queda estrictamente prohibido instalar software en los computadores y servidores sin las debidas autorizaciones. Los únicos autorizados para realizar instalación y desinstalación de programas, así como cambios de configuración en el sistema operativo son los encargados por la Proceso de Gestión de la Información.
e. Las equipos de cómputo no deben tener instalado ningún otro software que no sea el licenciado y requerido para que el usuario desarrolle su trabajo.

8.4. MANTENIMIENTO DEL EQUIPO DE CÓMPUTO.

El mantenimiento preventivo de los equipos se llevara acabo de las siguientes maneras correspondientes al tipo de mantenimiento preventivo.

a. La Proceso de Gestión de la Información es la encargada de gestionar que todo el equipo de cómputo de propiedad del hospital (computadores, computadores portátiles, y otros accesorios), sea actualizado tanto en hardware como en software, tendiendo a conservar e incrementar la calidad del servicio que presta.
b. Si el equipo de cómputo cambia de responsable se deberá notificar a la Proceso de Gestión de la Información para actualizar la hoja de vida del equipo.
c. Los responsables de las distintas áreas de los departamentos deberán dar cabal cumplimiento de las notificaciones correspondientes al Proceso de Gestión de la Información sobre la actualización, reubicación, etc. y todo aquello que implique movimientos en la ubicación de equipos de cómputo.

8.5. MANTENIMIENTO PREVENTIVO SEMESTRAL

Este mantenimiento se realizara de manera semestral siguiendo los pasos a continuación.

a. Se realizara la programación por parte de la proceso de Gestión de la Información.
b. Una vez realizado el mantenimiento de cada equipo se procede a su revisión por parte del usuario de que todo funcione correctamente y este dará su firma de conformidad dentro del formulario. Esta firma se realizara por cada usuario que reciba dicho mantenimiento.
c. Cuando se finaliza todo el mantenimiento se procede archivar el formulario y se procede a registrar el incidente en la Mesa de Ayuda.

Nota: El mantenimiento preventivo Semestral podrá realizarse o no, esto siendo determinado por la proceso de Gestión de la Información esto por motivo de que puede que los equipos no lo necesiten Ej. Equipos Nuevos

8.6. MANTENIMIENTO CORRECTIVO

Este mantenimiento se realiza cuando se presenten fallas de software y hardware dentro de los equipos de la ESE Hospital Universitario de la Samaritana y se procede a su reparación, siguiendo los siguientes pasos.

a. Se reporta a la sección de microinformática de la ESE Hospital Universitario de la Samaritana, acerca de algún problema.
b. Se levanta el incidente y se diligencia el formato.
c. Se procede a verificar el problema dentro del equipo.
d. Se procede al diagnóstico y reparación del equipo (En caso de que el equipo necesite alguna pieza que se pueda haber dañado esta se gestionara a través de la garantía si la tuviese de lo contrario se procede a realizar la gestión con el área de compras).
e. Se procede a la reparación del equipo.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

f. Se prueba la funcionabilidad del equipo por parte del al área de microinformática de la ESE Hospital Universitario de la Samaritana.
g. Se prueba la funcionabilidad del equipo por parte del usuario.
h. Una vez probado el equipo y si el usuario está satisfecho con el servicio se procede al cierre del incidente.

8.7. REUBICACIÓN DEL EQUIPO DE CÓMPUTO.

a. La reubicación del equipo de cómputo se realizará respetando los procedimientos que el Proceso de Gestión de la Información emita para ello.
b. Para reubicar un equipo de cómputo se debe contar con la autorización del responsable del proceso o servicio y del Proceso de Gestión de la Información, se verificará primero que el lugar hacia donde se trasladará disponga los medios necesarios para la instalación del equipo.
c. Si el área donde se va a reubicar el equipo de cómputo no cuenta con las condiciones mínimas para su funcionamiento y seguridad (Punto de red, corriente regulada, seguridad física) se deberá informar a la Proceso de Gestión de la Información mínimo 7 días antes de la reubicación para garantizar estas condiciones.

8.8. IMPRESORAS.

a. Se considera que un usuario hace mal uso de la impresora cuando imprime trabajos con fines diferentes a los administrativos.
b. Debe manipularse cuidadosamente las impresoras debido a que son fabricadas en su mayoría en plástico lo cual las hace muy delicadas.
c. Las hojas que se encuentren en el rodillo por ninguna razón se deben halar.
d. No se debe introducir hojas con clips, ganchos o grapas en la impresora.
e. Si la impresora comienza a emitir sonidos extraños, debe ser desconectada y sometida de inmediato a revisión para lo cual se notificará a la Proceso de Gestión de la Información.
f. Las impresoras NO tienen garantía por cartuchos/tóner.
g. Los usuarios por ningún motivo deben intentar desarmar una impresora ni intentar corregir atascos de papel, debe informar de inmediato a la empresa que se encuentra encargada de las impresoras Extensión 10716 y/o a la Proceso de Gestión de la Información para el caso de las impresoras TMU, para que se tomen las medidas pertinentes.
h. Los cambios de las partes o remplazo de las impresoras corren por parte de la empresa encargada de las mismas.

8.9. RECOMENDACIONES Y PRECAUCIONES.

i. El lugar de instalación debe ser un lugar ventilado, donde no esté expuesto directamente a los rayos solares, temperaturas extremas, humedad y polvo.
j. La superficie sobre la cual se van a instalar equipos debe ser totalmente plana y sin desniveles.
k. Se recomienda no instalar la CPU directamente en el piso, si no por el contrario se debe colocar sobre una base, más aun si es un tapete.
l. Por ningún motivo estando prendido el equipo deben ser tapados los sistemas de ventilación del mismo.
m. No colocar forros estando prendido el equipo.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

9. CONTROL DE ACCESO.

9.1. CONTROL DE LA INFORMACIÓN.

a. Los recursos disponibles a través de la red del Hospital serán de uso exclusivo para asuntos relacionados con las actividades propias del mismo.
b. Los usuarios deben informar inmediatamente a la Proceso de Gestión de la Información toda vulnerabilidad encontrada en la Red, aparición de virus o programas sospechosos, también se debe evitar al máximo distribuir ese tipo de información.
c. Para conectar cualquier equipo a la Red se debe tener autorización explícita de la Proceso de Gestión de la Información.
d. Los usuarios nunca deben intentar sobrepasar los controles de los sistemas, intentar examinar los computadores o las redes de la entidad en busca de archivos de otros usuarios sin su autorización o implantar software diseñado para causar daño.
e. Los usuarios no deben suministrar ningún tipo de información a externos sin las autorizaciones respectivas, esto incluye los controles de sistemas de información y su respectiva implementación.
f. Los usuarios no deben consultar, destruir, modificar, copiar o distribuir los archivos de la entidad sin los permisos respectivos.
g. Todo usuario que utilice los recursos de los sistemas y de Red tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad de la información que maneje; especialmente si dicha información se ha clasificado como crítica.
h. Los usuarios no deben usar los equipos para asuntos personales a menos que exista una autorización respectiva que evalúe el riesgo informático de tal labor.
i. Las carpetas compartidas en la Red del hospital a las cuales todos los usuarios tengan permiso de lectura o escritura no deben contener información sensible del hospital, en caso de ser así la carpeta compartida debe estar configurada para que solo accedan a ella únicamente los usuarios autorizados.

9.2. CONTROL DE ACCESO LOCAL A LA RED.

a. La Proceso de Gestión de la Información es responsable de proporcionar a los usuarios el acceso a los recursos informáticos a través del uso de nombre de usuario y contraseña.
b. La Proceso de Gestión de la Información verificará el uso responsable acorde con los lineamientos de seguridad informática del hospital.
c. El acceso lógico a equipos especializados de cómputo (servidores, enrutadores, bases de datos, Access Point, switches, etc.) conectados a la red son directamente administrados por la Proceso de Gestión de la Información.
d. Todo equipo de cómputo que esté conectado a la Red o aquellos que en forma autónoma se tengan, deben sujetarse a los procedimientos de acceso que emite la Proceso de Gestión de la Información.

9.3. CONTROL DE ACCESO REMOTO.

a. La Proceso de Gestión de la Información es responsable de proporcionar el servicio de acceso remoto y de brindar el acceso a los recursos informáticos disponibles con las medidas de seguridad que estime necesarias, en caso especial de acceso a los recursos de los servidores del hospital por terceros, estos deberán ser autorizados por la Gerencia y la Proceso de Gestión de la Información.
b. El usuario de estos servicios deberá sujetarse a los reglamentos de uso de la Red del hospital y los lineamientos generales de uso de Internet.
c. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la Proceso de Gestión de la Información.
d. Todo acceso se deberá realizar por VPN a través de un usuario y contraseña asignado por la Proceso de Gestión de la Información previo acuerdo.
e. El Uso de clientes de acceso remoto como team viewer u otros con las mismas características se encuentran restringidos.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

9.4. ACCESO A LOS SISTEMAS DE INFORMACIÓN.

a. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la Proceso de Gestión de la Información.
b. El manejo de información asistencial y administrativa que se considere restringida deberá ser cifrada con el objeto de conservar su integridad.
c. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red del hospital y por las normas y procedimientos establecidos por el Proceso de Gestión de la Información.
d. Los servidores de bases de datos son dedicados, por lo que se prohíben los accesos a usuarios, excepto para el personal autorizado por la Proceso de Gestión de la Información.
e. El control de acceso a cada sistema de información será determinado de acuerdo con la unidad responsable de generar y procesar los datos involucrados.

9.5. ACCESO A LOS SISTEMAS INFORMÁTICOS DEL HOSPITAL (SOFTWARE)

a. El acceso a los diferentes aplicativos que se tienen en el hospital deben ser solicitados a través del formato de activación e inactivación de usuarios, (Ver procedimiento de activación e inactivación de usuarios)
b. Los usuarios son responsables de todas las actividades llevadas a cabo con sus cuentas en los diferentes aplicativos del hospital.
c. El código de acceso será informado, este depende del aplicativo al que se le creo usuario.
d. El control de acceso a los aplicativos será determinado de acuerdo a la unidad responsable de generar y procesar los datos involucrados.
e. El líder de proceso reportara a la proceso de Gestión de la Información cuando se produzcan vacaciones, licencias, retiro, traslado; quienes procederán a realizar las acciones correspondientes.

9.6. CONTENIDO PÁGINA WEB E INTRANET DEL HUS.

a. El material que aparezca publicado en la página de Internet del hospital deberá ser enviado aprobado por el Comité de Comunicaciones, la Gerencia y a la Proceso de Gestión de la Información, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
b. El material que aparezca en la Intranet del hospital deberá ser aprobado por el líder de proceso del material a publicar y debe estar de acuerdo con las normas y procedimientos establecidas por la Proceso de Gestión de la Información.
c. El software creado por el proceso de gestión de la información del Hospital puede ser protegido jurídicamente desde la propiedad intelectual, industrial (patente) o los derechos de autor.
d. La protección que la ley colombiana otorga al Derecho de Autor se realiza sobre todas las formas en que se puede expresar las ideas, no requiere ningún registro y perdura durante toda la vida del autor, más 80 años después de su muerte, después de lo cual pasa a ser de dominio público. El registro de la obra ante la Dirección Nacional del Derecho de Autor sólo tiene como finalidad brindar mayor seguridad a los titulares del derecho.
e. En el caso del Software, la legislación colombiana lo asimila a la escritura de una obra literaria, permitiendo que el código fuente de un programa esté cubierto por la ley de Derechos de Autor.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

10. SOFTWARE.

9.7. ADQUISICIÓN DE SOFTWARE.

a. Acorde con los lineamientos de la institución, el proceso de gestión de la información es el proceso oficial del hospital encargado para establecer los mecanismos de administración de los sistemas informáticos.
b. El proceso de gestión de la información propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y de licencias en cantidad en busca de obtener economías a escala.
c. Corresponde al proceso de gestión de la información emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia así como el verificar que el software provenga de fuentes conocidas y seguras.
d. La Proceso de Gestión de la Información deberá promover el uso de sistemas informáticos que redunden en la independencia de la Institución para con los proveedores.

9.8. INSTALACIÓN DE SOFTWARE.

a. Corresponde al proceso Gestión de la Información emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
b. En los equipos de cómputo, telecomunicaciones y en dispositivos basados en sistemas de cómputo únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde.
c. La Proceso de Gestión de la Información es responsable de brindar asesoría y supervisión para la instalación de software informático, asimismo para el software de telecomunicaciones.
d. La instalación de software que desde el punto de vista de la Proceso de Gestión de la Información pueda poner en riesgo los recursos de la institución no está permitida.
e. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, firewalls, privilegios de acceso y otros que se apliquen).

9.9. ACTUALIZACIÓN DE SOFTWARE.

a. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al cronograma que anualmente sea propuesto por la Proceso de Gestión de la Información.
b. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la Proceso de Gestión de la Información.

9.10. AUDITORIA DE SOFTWARE INSTALADO.

a. La Proceso de Gestión de la Información y la Oficina Asesora de Control Interno son los responsables de realizar revisiones periódicas para asegurar que sólo el software con licencia esté instalado en los computadores del hospital.
b. La Proceso de Gestión de la Información está autorizada para realizar auditorías en los sistemas de cómputo y sistemas de información.
c. Corresponderá a la Proceso de Gestión de la Información y a la Oficina Asesora de Control Interno dictar las normas, procedimientos y calendarios de auditoria.

9.11. SOFTWARE PROPIEDAD DE LA INSTITUCIÓN.

a. Todo el software adquirido por el hospital sea por compra, donación o sesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

le confiera.

b. La Proceso de Gestión de la Información en coordinación con la Oficina Asesora de Control Interno deberá tener un registro de todo el software propiedad del hospital.
c. Todos los sistemas de software (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del hospital se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.
d. El concepto de "propiedad intelectual", acogido por el artículo 61 de la Constitución Política, en concordancia con el artículo 2 numeral 8 del Convenio que establece la Organización Mundial de la Propiedad Intelectual, es omnicomprensivo de diferentes categorías de propiedad sobre creaciones del intelecto, que incluye dos grandes especies o ramas: la propiedad industrial y el derecho de autor, que aunque comparten su naturaleza especial o sui generis, se ocupan de materias distintas. Mientras que la primera trata principalmente de la protección de las invenciones, las marcas, los dibujos o modelos industriales, y la represión de la competencia desleal, el derecho de autor recae sobre obras literarias, artísticas, musicales, emisiones de radiodifusión, programas de Computador, etc., por esta razón todos los sistemas de software (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del hospital serán amparados por los derechos de autor, (Ver punto 9.7).
e. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.
f. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.
g. La Proceso de Gestión de la Información en conjunto con la Dirección Administrativa propiciará la gestión de patentes y derechos de creación de software propiedad de la institución.
h. La Proceso de Gestión de la Información administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la lineamiento informática del Hospital.

9.12. USO DE SOFTWARE ACADÉMICO.

- Cualquier software que requiera ser instalado para trabajar sobre la Red del hospital deberá ser evaluado por el Proceso de Gestión de la Información y deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución.

9.13. PROPIEDAD INTELECTUAL.

- Corresponde a la Proceso de Gestión de la Información procurar que todo el software instalado en el hospital esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

10. INTERNET.

10.1. ASIGNACIÓN DE INTERNET.

a. El Proceso de Gestión de la Información y la Gerencia del hospital se reservan el derecho de asignar el servicio de Internet, previa evaluación de la necesidad expresada

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

por el solicitante y la disponibilidad de recursos existentes.

b. El acceso a Internet debe solicitarse mediante el diligenciamiento del formato de activación de usuarios, seleccionando la opción de internet. Esta comunicación debe estar firmada por el líder de proceso correspondiente al usuario que hace la solicitud.
c. La autenticación para el servicio de Internet (usuario y contraseña) será igual a la utilizada para el usuario del dominio HUS.
d. Se asignara el nivel de navegación dependiendo el rol que desempeñe.

10.2. USO PERMITIDO.

a. El uso de Internet es exclusivamente para las actividades institucionales. El uso de Internet para asuntos personales se permite siempre y cuando su utilización sea por tiempo limitado y esté de acuerdo con lineamientos del uso del Internet y no influya de manera negativa en el desempeño de las tareas y responsabilidades para con la Institución. El uso personal puede ser negado en casos en los que se haga uso excesivo de los recursos del canal de Internet.
b. Los usuarios utilizaran únicamente los servicios para los cuales están autorizados. No deberán utilizar el equipo de otra persona o intentar apoderarse de claves de acceso de otros, así como no deberán acceder y modificar archivos que no son de su propiedad y mucho menos los pertenecientes al hospital o a otras Instituciones.
c. Está totalmente prohibido para forzar el ingreso a páginas de contenidos sexuales, racistas o cualquier otro tipo de material ofensivo, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material ya sea vía Web o medios magnéticos. Los funcionarios que accidentalmente se conecten a páginas de Internet que tengan estos contenidos deben desconectarse inmediatamente e informar a la Proceso de Gestión de la Información para que estos accesos sean bloqueados.
d. Está prohibido descargar música o video, participar en juegos de entretenimiento en línea o utilizar los servicios de Radio y TV por demanda.
e. Está prohibido la descarga, instalación y uso de programas ajenos al licenciamiento del hospital ya sea software libre (freeware o shareware), toolbars, hotbars, messenger o cualquier otra acción que altere las configuraciones ya instaladas en los computadores, cualquier necesidad deberá ser consultada con la Proceso de Gestión de la Información.
f. Los accesos desde el exterior a través de Internet para utilizar el sistema de información del hospital o cualquier otra aplicación en forma remota y en tiempo real deben ser autorizados por el Proceso de Gestión de la Información y la Gerencia.

10.3. SEGURIDAD.

a. Cualquier archivo descargado a través de Internet debe revisarse con un antivirus para garantizar que no contenga virus, hardware, spyware o código malicioso. Estos virus pueden comprometer la seguridad del hospital, afectar el funcionamiento tanto de los computadores como del rendimiento de la red o hasta destruir la información del disco duro del computador. Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que sea un archivo confiable. Todo equipo con acceso a Internet debe tener instalado un antivirus con sus bases de datos actualizadas y siempre debe estar activo.
b. El nivel de seguridad del navegador de Internet debe estar configurado con un nivel medio-alto. De esta forma se controla la ejecución de secuencias de comandos, componentes, controles y complementos ActiveX provenientes de sitios de alto riesgo que puedan dañar o comprometer la información en el computador. También de esta forma se controla la descarga automática de archivos y el bloqueo de menús emergentes.
c. Está prohibido hacer uso de los servicios de Internet para interferir en los sistemas de información o intentar burlar los sistemas de seguridad propios del hospital.
d. Si se retira de su puesto de trabajo por un periodo de tiempo deberá bloquear su sesión de usuario, si va a dejar de usarlo permanentemente cierre todas las aplicaciones y apague el equipo.
e. Si sospecha que su contraseña ha sido violada deberá informar inmediatamente a la Proceso de Gestión de la Información para realizar el cambio de la misma.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

f. Todos los archivos de ingreso son inspeccionados por los módulos anti-spam y control de contenido si resultan sospechosos o que representen algún riesgo serán bloqueados y por este motivo no serán entregados al destinatario.
g. El uso de memorias USB se encuentra restringido y solo podrá hacer uso del mismo personal autorizado por la Proceso de Gestión de la Información.
h. Toda la red del Hus se encuentra administrada por la solución Firewall de última generación por tal motivo todo el tráfico es evaluado constantemente y el comportamiento mal intencionado y reiterativo de un usuario será reportado al Líder del área para que se tomen las medidas pertinentes.
i. Para cambios De contraseñas el funcionario debe acercarse a la proceso de Gestión de la Información con su respectiva identificación para realizar el respectivo trámite.
j. Todo equipo externo que por algún motivo sea necesario ser conectado a la red del Hus debe ser autorizado por la proceso de Gestión de la Información.
k. Después de tres intentos fallidos de autenticación la cuenta se bloqueara por cinco minutos.
l. Todos los equipos del Hus se encuentran sincronizados con un servidor de actualizaciones (WSUS), es necesario que el funcionario permita la instalación de las mismas al apagar el equipo y no interrumpirlas ya que estas son de gran importancia en la seguridad y funcionamiento del Equipo.
m. Dado el caso que el sistema de intrusiones del Hus (ISP) detecte y envié alerta de algún equipo de la red se encuentra realizando tareas sospechosas, el Funcionario debe facilitar el equipo de manera oportuna para el análisis con el fin de no exponer la seguridad y la información de la entidad.

11. GENERALES.

11.1. SUPERVISIÓN Y EVALUACIÓN.

a. La Proceso de Gestión de la Información podrá monitorear las actividades de los usuarios tanto en las actividades relacionadas con los sistemas de información, el uso de la red, el correo electrónico institucional y el servicio de Internet mediante un Log de auditoria para garantizar el cumplimiento de las lineamientos de seguridad y de esta forma se evitará el riesgo a la seguridad de la operación, servicio y funcionalidad del sistemas informático del hospital.
b. Para efectos de confiabilidad el hospital podrá realizar un monitoreo sobre todos y cada uno de los servicios informáticos. Los sistemas críticos estarán monitoreados permanentemente.

11.2. RESPONSABILIDADES.

a. Cada uno de los usuarios del hospital es responsable del cumplimiento de los lineamientos aquí establecidos y los líderes de proceso deberán supervisar el cumplimiento de los mismos.
b. Toda información confidencial del hospital, relacionada con los sistemas de información, deberá ser tratada bajo estricta seguridad y el personal a cargo no está autorizado a revelarlo a terceros.

11.3. SANCIONES.

a. El incumplimiento de los lineamientos aquí expuestos puede acarrear consecuencias, tales como: la cancelación temporal de la cuenta del usuario del dominio, cuenta de correo, cuenta de Internet, y en algunos casos la suspensión definitiva de la misma.
b. Las sanciones pueden ser desde una llamada de atención, informar al usuario o hasta la suspensión del servicio dependiendo de la gravedad de la falta o de la malicia que manifieste.
c. En otros casos se analizará el caso en particular y se adoptaran las medidas pertinentes.

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

d. Todas las acciones en las que se comprometa la seguridad de los sistemas informáticos del HUS y que no estén previstas en esta lineamiento serán sancionados.

12. LINEAMIENTOS GENERALES DE ALMACENAMIENTO DE INFORMACIÓN

12.1. INTRODUCCIÓN.

El término lineamiento de almacenamiento de la información se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos que indican en términos generales que está y que no está permitido en el área de almacenamiento durante la operación general de dicho sistema.

Estos lineamientos conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas y son parte importante del sistema de seguridad que la organización posee para salvaguardar sus activos informáticos.

El objetivo de la lineamiento de almacenamiento de información es dar a conocer y oficializar entre los usuarios de sistemas informáticos de la E.S.E. Hospital Universitario de la Samaritana, el modelo de almacenamiento de información que aplica a los servicios basados en plataformas informáticas, ofrecidos por el hospital.

Los lineamientos de almacenamiento de información constituyen la posición oficial de la Gerencia y la Proceso de Gestión de la Información en relación con la seguridad de la infraestructura y sistemas informáticos del hospital. Su cumplimiento por parte de los usuarios de la Red del hospital es de carácter obligatorio, en ella se ofrece de manera respetuosa y cortesa las normas y procedimientos con el fin de garantizar el buen funcionamiento de la institución. El desconocimiento del mismo no exonera a la persona de las responsabilidades asignadas.

12.2. SEGURIDAD FÍSICA.

El servidor de almacenamiento está ubicado en el centro de cómputo del HUS, al cual solo pueden acceder usuarios autorizados de sistemas, que cuentan con una tarjeta de acceso y que tienen su huella registrada en el sistema biométrico de control de acceso.

12.3. RESPALDO DE LA INFORMACIÓN.

La E.S.E. Hospital Universitario de la Samaritana cuenta con un sistema de almacenamiento. En este servidor de almacenamiento denominado servidor de archivos, que cuenta con espacio disponible se encuentra recurso de red compartidos para cada una de las unidades funcionales del hospital. Los usuarios deben realizar en el servidor de almacenamiento copia de la información que requiera de un respaldo por el grado de importancia.

12.4. FLUJO DE LA INFORMACIÓN.

Los usuarios de las diferentes áreas son responsables de realizar copias de seguridad de la información de sus computadores al menos una vez a la semana en el servidor designado para tal fin.

12.5. CONTROL DE PERSONAL.

Solo podrán acceder a los recursos compartidos usuarios autenticados en el Dominio HUS y debidamente autorizados en los permisos que se concedan directamente sobre el recurso compartido. Los jefes de sus respectivas área son los responsables de informar a la Proceso de Gestión de la Información sobre qué usuarios se les debe permitir

5. RELACION DE LOS PROCEDIMIENTOS E INTERACCION ENTRE ELLOS

acceso al recurso compartido para almacenar copias de seguridad de igual manera a quienes se les debe revocar por retiro de la institución o traslado a otra dependencia.

12.6. CONTROL DE TERCEROS.

Ninguna persona externa al hospital podrá tener acceso a los recursos compartidos en la red para proteger la confidencialidad y evitar el robo de la información.

12.7. TIPO DE INFORMACIÓN.

Las copias de seguridad llevadas al servidor de respaldos solo pueden contener documentos relacionados con actividades concernientes con su labor en la institución.
Por ningún motivo se aceptan archivos de tipo música, videos, fotografías.
El espacio inicialmente asignado para cada usuario es de 10 Gb y solo se puede incrementar con solicitud dirigida por el Proceso de Gestión de la Información plenamente justificada.

13. CONTROL DE LA INFORMACIÓN.

a. Los recursos disponibles a través de la Red del hospital serán de uso exclusivo para asuntos relacionados con las actividades propias del hospital.
b. Los usuarios deben informar a la Proceso de Gestión de la Información sobre cualquier vulnerabilidad encontrada en la Red, aparición de virus o programas sospechosos, también debe evitar al máximo distribuir este tipo de información interna o externamente.
c. Los usuarios nunca deben intentar sobrepasar los controles de los sistemas, intentar examinar los computadores y redes de la entidad en busca de archivos de otros usuarios sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.
d. Los usuarios no deben consultar, copiar, modificar, destruir o distribuir los archivos de la entidad sin los permisos respectivos.
e. Todo usuario que utilice los recursos de los sistemas y de Red, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad y auditabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.
f. Las carpetas compartidas en la Red del hospital a las cuales todos los usuarios tengan permiso de lectura o escritura no deben contener información sensible del hospital, en caso de ser así la carpeta compartida debe estar configurada para que solo accedan a ella únicamente los usuarios autorizados.
g. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.
h. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados
i. Corresponde a la Proceso de Gestión de la Información promover y difundir los mecanismos de respaldo (back-up) y salvaguarda de los datos y del software que se encuentre en el servidor de almacenamiento.

6. BIBLIOGRAFIA

- Sobre Derecho de Autor en Colombia, en la Oficina Nacional de Derecho de Autor: http://www.derechodeautor.gov.co/
- Colombia, Congreso de la República. (1982, Enero 28). Ley 23 de 1982: sobre derechos de autor. Bogotá: Diario oficial. Consultado en abril de 2012, de http://www.alcaldiabogota.gov.co/sisjur/
- Colombia, Presidente de la República. (1989, Junio 23). Decreto 1360 de 1989: Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. Bogotá: Diario oficial. Consultado en abril de 2012, de http://www.alcaldiabogota.gov.co/sisjur/

7. CONTROL DE CAMBIOS

VERSION	FECHA	ITEM MODIFICADO	JUSTIFICACION
01	23/05/2016	N/A	Viene del manual 01SI02 – V2 seguridad informática