

GESTIÓN DE INFORMACIÓN

Edición N°: 3

Revisión N°: 2

Fecha: Junio de 2017

Fecha: Enero de 2020

Responsable: Jefe de Gestión de la Información

Área: Gestión de la Información

REGLAMENTO DE SEGURIDAD INFORMATICA

Manuel Uribe Angel

E.S.E HOSPITAL

Vinculados con la Vida!

Elaboró: Oscar Cano Villa – Técnico Operativo
de Gestión de la Información

Aprobó: Martha Lucía Vélez Arango
Gerente

Firma:

Firma:

HOJA DE CONTROL DEL DOCUMENTO

EDICIÓN	REVISIÓN	FECHA	ELABORÓ	REVISÓ	APROBÓ	OBSERVACIONES
1		Febrero de 2009	Gloria Pineda	Grupo de Mejoramiento del sistema de información	Juan Guillermo Tamayo Maya	
2		Septiembre de 2014	Grupo de Sistemas de Información	Jefe de Sistemas de Información	Martha Lucía Vélez Arango	
3		Junio de 2017	Oscar Cano Villa	Jefe de Sistemas de Información	Martha Lucía Vélez Arango	
3	1	Agosto de 2019	Oscar Cano Villa	Jefe de Sistemas de Información	Martha Lucía Vélez Arango	Se actualiza la gestión de contraseñas.
3	2	Enero de 2020	Oscar Cano Villa	Jefe de Sistemas de Información	Martha Lucía Vélez Arango	Ajuste en el manejo de contraseñas

**Resolución Número 094
(8 de mayo de 2009)**

Por medio de la cual deroga las resoluciones anteriores relacionadas con la Gestión del Sistema de la Información de la ÉSE Hospital Manuel Uribe Ángel y adopta los documentos actualizados y los nuevos documentos, los cuales son: PESI Plan Estratégico del Sistema de Información, Plan de Contingencia del Sistema de Información, Manual Interno de Seguridad Informática, Modelo del sistema de información, Reglamento de Seguridad Informática, Metodología para la selección del tamaño de muestra y de las unidades muestrales, Campaña para Mejorar la Calidad del Dato, Instructivo de Estadística, Metodología para la Detección de Necesidades del Sistema de Información y Manual de Historia Clínica

El Gerente de la ESE Hospital Manuel Uribe Ángel Envigado, en uso de sus atribuciones legales y estatutarias y

CONSIDERANDO

- Que La ESE Hospital Manuel Uribe Ángel, consciente el camino hacia la mejoramiento de la calidad organizacional se basa en el uso eficiente, estratégico y funcional de la información, con el propósito de gerenciar la información en la organización de manera precisa y confiable hacia la estrategias administrativas que favorezcan la integralidad hacia a los objetivos institucionales; mediante la estandarización, integración, consolidación, análisis y retroalimentación de la información.
- Que la ESE considera necesario contar con lineamientos claros que permitan encaminar los esfuerzos institucionales hacia el desarrollo de un sistema de información moderno y eficaz, que permitan disponer de información confiable y oportuna para la toma de decisiones y para interactuar en forma eficaz y eficiente con el sistema de salud.
- Que para que el sistema de información cumpla con su objetivo es necesario que la información generada sea oportuna, confiable, segura y disponible; por tanto se requiere generar un modelo de sistema de información que permita visualizar la gestión de la información de la ESE teniendo en cuenta que cada uno de los procesos de la institución deberá pasar por le ciclo de vida de la información.
- Que La ESE considera que es necesario divulgar a los usuarios de la red informática acerca de sus obligaciones, instrucciones y prácticas recomendadas en el cumplimiento del buen manejo del hardware y el

software en el Hospital y para hacer uso adecuado de las herramientas que el sistema de información tiene a su disposición.

- Que con el fin de garantizar la seguridad de la información del usuario considera importante la aplicación y mejora continua de un conjunto procedimientos de seguridad para el manejo de la historia clínica.
- Que se hace necesario contribuir a mejorar la calidad de la información generada en la institución a través de la recopilación adecuada de los datos: en el registro inicial, el procesamiento y análisis periódico garantizando información completa y confiable que pueda reorientar no sólo la dirección de las acciones de control, sino también sugerir la toma de medidas o estrategias nuevas.

RESUELVE

Artículo Primero: adóptese y cúmplase con los lineamientos descritos en los siguientes documentos: PESI Plan Estratégico del Sistema de Información, Plan de Contingencia del Sistema de Información, Manual Interno de Seguridad Informática, Modelo del sistema de información, Reglamento de Seguridad Informática, Metodología para la selección del tamaño de muestra y de las unidades muestrales, Campaña para Mejorar la Calidad del Dato, Instructivo de Estadística, Metodología para la Detección de Necesidades del Sistema de Información y Manual de Historia Clínica

Dado en Envigado el día 8 del mes de mayo de 2009.

JUAN GUILLERMO TAMAYO MAYA
Gerente

CONTENIDO

1. INTRODUCCIÓN	6
2. OBJETIVO.....	6
3. RESPONSABLES	6
4. DEFINICIÓN	6
5. REGLAMENTO SOBRE EL USO DE LA TECNOLOGÍA.....	7
5.1. CUMPLIMIENTO LEY 603 DE 2000.....	7
5.2. BUEN MANEJO DEL INSUMO INFORMÁTICO	7
5.3. ESTÁNDAR DE FIRMA DE CORREOS INSTITUCIONALES.....	7
5.4. ESTÁNDAR DE CONTENIDO PARA CORREOS INSTITUCIONALES	8
5.5. REPORTE NOVEDAD INGRESO/RETIRO USUARIOS	8
5.6. CONTROL DE IMPRESIÓN Y RACIONALIZACIÓN DEL COSTO DE IMPRESIÓN	9
5.7. ASIGNACIÓN RECURSOS INFORMÁTICOS A TERCEROS.....	9
5.8. SERVICIO DE INTERNET EN HABITACIONES DE PACIENTES.....	9
5.9. ASIGNACIÓN ANTIVIRUS AL 100% SERVIDORES Y PC	9
5.10. CREACIÓN Y CONEXIÓN CENTROS DE CABLEADO	10
5.11. REPORTE MAL USO RECURSOS INFORMÁTICOS	10
6. RESPONSABILIDADES DEL USUARIO	10
6.1. GARANTIZAR USB LIBRES DE VIRUS	10
6.2. GESTIÓN DE CONTRASEÑAS	10
6.3. CONTENIDO DE LOS MENSAJES INSTITUCIONALES	13
6.4. CUSTODIA INSUMOS INFORMÁTICOS Y CONTROL DE ENERGÍA DE MONITORES Y COMPUTADORES.....	13
6.5. CUSTODIA INSUMOS INFORMÁTICOS PARA USO EXCLUSIVO DE ACTIVIDADES LABORALES	13
6.6. GARANTIZAR LEGALIDAD DEL SOFTWARE EN EL EQUIPO ASIGNADO	14
6.7. NO ATENTAR CONTRA INSUMO INFORMÁTICO	14
6.8. RESPONSABILIDAD DE LAS COPIAS DE SEGURIDAD	14
6.9. NOTIFICAR ANOMALÍAS EN EL CUIDADO INSUMOS INFORMÁTICOS.....	14
7. ACTIVIDADES NO AUTORIZADAS AL USUARIO	15
7.1. MANIPULACIÓN DE INFORMACIÓN	15
7.2. MENSAJES PÚBLICOS	15
7.3. RECURSOS INFORMÁTICOS PARA ACTIVIDADES PERSONALES	15
7.4. EXCEDER CUOTA BUZÓN DE MENSAJES	15
7.5. ENVÍO MENSAJES NO INSTITUCIONALES	15
7.6. RED EXCLUSIVA PARA PROPÓSITOS LABORALES	16
7.7. INGRESO PERSONAL NO AUTORIZADO A LA OFICINA DE GESTIÓN DE INFORMÁTICA Y/O CENTRO DE CÓMPUTO	16
7.8. CAMBIO CONFIGURACIÓN ESTACIÓN DE TRABAJO.....	17
7.9. MOVER FÍSICAMENTE LOS INSUMOS INFORMÁTICOS DEL PUESTO DE TRABAJO	17
7.10. USO DE RECURSOS INFORMÁTICOS EN HORARIO NO LABORAL SEGÚN EL CARGO	17
7.11. USO DE OBJETOS NO ACORDES A LA FUNCIÓN DEL INSUMO INFORMÁTICO	17
7.12. INTERCAMBIO DE INSUMOS INFORMÁTICOS QUE ALTEREN EL INVENTARIO DE HARDWARE.....	17
8. REGLAMENTACIÓN PARA NO USUARIOS DE LA EN LA E.S.E HOSPITAL MANUEL URIBE ÁNGEL Y SUS SEDES.	18
9. FALTAS CON TRÁMITE DISCIPLINARIO	18
10. RESPONSABILIDAD DEL PROVEEDOR DE OUTSOURCING DE TI	19
11. SANCIONES.....	19
11.1. SERVIDORES PÚBLICOS	19
11.2. CONTRATISTAS	19
11.3. AUDITORES MÉDICOS	19

1. INTRODUCCIÓN

La E.S.E Hospital Manuel Uribe Ángel Ofrece a sus clientes internos acceso a su infraestructura tecnológica como herramienta de trabajo en actividades laborales y de investigación que se llevan a cabo dentro de las instalaciones de la institución. El acceso se hace a través de computadores utilizando la red local de la E.S.E Hospital Manuel Uribe Ángel y sus sedes que permite que los diferentes usuarios utilicen una serie de servicios como Software de Gestión Hospitalaria y Administrativa, navegación en Internet, Intranet, correo web, transferencia de archivos, servicio de impresión, unidades compartidas, y acceso a los demás aplicativos institucionales. Por tanto; es necesario divulgar a los usuarios de la red informática acerca de sus obligaciones en el cumplimiento de las mejores prácticas y el buen manejo del hardware y el software en el Hospital, para hacer uso adecuado de dichas herramientas.

2. OBJETIVO

- Definir el reglamento de uso de recursos Informáticos en la E.S.E Hospital Manuel Uribe Ángel y sus sedes, las implicaciones que estas tienen en caso de una inadecuada utilización.

3. RESPONSABLES

Los responsables de la actualización de los manuales, instructivos y formatos inmersos en el presente manual son la Jefe de Gestión de la Información y el Analista de Infraestructura de la E.S.E Hospital Manuel Uribe Ángel

4. DEFINICIÓN

Usuario de la red informática: Este concepto cobija a todos los clientes internos, auditores médicos, miembros de empresas de outsourcing, visitantes, médicos de prácticas, estudiantes de práctica, pacientes o representantes de convenios que utilicen la red de la institución o un computador externo previamente autorizado por escrito para ser conectado dentro de las instalaciones de la E.S.E Hospital Manuel Uribe Ángel y sus sedes por un periodo determinado.

5. REGLAMENTO SOBRE EL USO DE LA TECNOLOGÍA

5.1. Cumplimiento Ley 603 de 2000

Es iniciativa de la E.S.E Hospital Manuel Uribe Ángel informar y educar sobre los beneficios que trae la legalidad para el país, la economía y la productividad de las empresas, recuerda que la defraudación a los Derechos Patrimoniales de Autor es un delito que tiene sanciones, pero es la responsabilidad de cada representante Legal el cumplimiento de la Ley 603 de 2000.

Las leyes que protegen en Colombia el Derecho de Autor, se encuentran el artículo 271 del Código Penal, que protege los Derechos Patrimoniales de Autor, y el 272, que sanciona la violación a los mecanismos de seguridad que protegen al software. Estos artículos establecen penas de 4 a 8 años de prisión y de 26,66 a 1000 salarios mínimos legales mensuales vigentes.

Particularmente para el caso del software, es necesario que las empresas proveedores de servicios de la E.S.E Hospital Manuel Uribe Ángel que cuentan con PC instalados dentro de la Red de la E.S.E Hospital Manuel Uribe Ángel y sus sedes anexas a sus contratos la declaración del estado de cumplimiento en la materia, se aseguren que todos los programas instalados en las compañías que representan y que se encuentran al servicio de la E.S.E Hospital Manuel Uribe Ángel cuentan con las respectivas licencias, legalmente adquiridas y debidamente certificadas.

El compromiso de cada usuario es el compromiso de toda la institución. Por lo tanto, cualquier instalación de software dentro de E.S.E Hospital Manuel Uribe Ángel y sus sedes debe ser aprobada por el área de Gestión de la Información.

5.2. Buen manejo del Insumo Informático

Cada usuario debe conocer este reglamento y la correspondiente responsabilidad por sus acciones, al utilizar un insumo informático como PC, Servidor, Impresora, etc., dentro de las instalaciones de la E.S.E Hospital Manuel Uribe Ángel y sus sedes, acceder a la red o al Internet, a través de la infraestructura tecnológica construida exclusivamente para los servicios administrativos y asistenciales que ofrece la E.S.E.

5.3. Estándar de firma de correos institucionales

Se solicita utilizar el estándar para la firma de correos, personalizada para cada usuario de acuerdo a la sede donde este se encuentre, cuando el buzón sea genérico llevará el nombre del área que representa. Ejemplo:



Nombre Completo | Cargo | buzon@hospitalmua.com.co |
www.hospitalmanueluribeangel.gov.co | E.S.E. Hospital Manuel
Uribe Ángel - Diagonal 31 N° 36 A Sur 80. Envigado, Colombia |
Tel(s): (+57 4) 3394800 Ext.

Antes de imprimir este correo, asegúrese de que sea necesario.
Vinculados con la Vida!



Nombre Completo | Cargo | buzon@hospitalmua.com.co |
www.hospitalmanueluribeangel.gov.co | E.S.E. Hospital Manuel
Uribe Ángel – Sede - Dirección. Envigado, Colombia | Tel(s): (+57
4) 4489400 Ext.

Antes de imprimir este correo, asegúrese de que sea necesario.
Vinculados con la Vida!

5.4. Estándar de Contenido para Correos Institucionales

Todo mensaje enviado por un usuario debe incluir un encabezado o título del mensaje, nombre, cargo y teléfono con extensión, también se puede incluir la firma como configuración.

En los casos en que el correo electrónico sea compartido por varios usuarios, se debe incluir un encabezado o título del mensaje, nombre, cargo y teléfono con extensión, no se debe configurar con la firma digital.

Es responsabilidad del usuario depurar su buzón de correo, no dejarlo llenar, el área de soporte técnico no se hace responsable de la pérdida de los mensajes por mal manejo de parte de los usuarios.

5.5. Reporte Novedad Ingreso/Retiro Usuarios

Al momento del ingreso o retiro de un usuario de la institución, el área de Talento Humano de la E.S.E Hospital Manuel Uribe Ángel debe notificar inmediatamente vía email que le asignen o reciban según sea ingreso o retiro el inventario tecnológico asignado a ese usuario y que bloquee o cancele la cuenta y clave(s) que tiene asignada. La seguridad de la información debe garantizarse con un proceso oportuno de reporte de ingreso y retiro de usuarios en la red y/o aplicativos institucionales.

Cualquier ingreso de un usuario debe anexar el respectivo CDP en caso de compra de insumos informáticos o el licenciamiento respectivo de acuerdo al cargo a realizar.

5.6. Control de Impresión y racionalización del costo de Impresión

Todo usuario tiene derecho a hacer uso de los servicios de impresión, siempre y cuando tenga relación con labores de la E.S.E Hospital Manuel Uribe Ángel y sus sedes, es decir, que el documento a imprimir esté relacionado con el objeto de las funciones a su cargo o de su contrato. La estrategia de reducción de costos de impresión es responsabilidad de cada usuario que tiene asignado un servicio de impresión garantizando impresión en baja calidad y solo de los documentos que ameriten para garantizar campañas de control de impresión.

5.7. Asignación Recursos Informáticos a Terceros

La E.S.E Hospital Manuel Uribe Ángel por ser una Empresa Social del Estado no podrá beneficiar tecnológicamente a ningún tercero, si el tercero desea utilizar los servicios de la E.S.E Hospital Manuel Uribe Ángel y sus sedes, deberá cancelar el valor requerido del uso de la tecnología, por ejemplo, licencias de red, licencias de antivirus, licencias de aplicativos y herramientas de Office, uso de servicios de impresión, uso de puntos de switches, acceso a Internet, correo electrónico institucional entre otros.

5.8. Servicio de Internet en Habitaciones de Pacientes

La E.S.E Hospital Manuel Uribe Ángel ofrece el servicio de Navegación a Internet a las siguientes zonas comunes y habitaciones (Torre2 Piso2 “Servicio Privado” y auditorio, Sala espera Cirugía y Urgencias, Sala de Juntas, Torre 2 piso 1 (Oncología) y Auditoria, como valor agregado en función del servicio ofrecido por el área de Mercadeo. Con restricción de navegación, con un usuario y clave asignado de manera general.

5.9. Asignación Antivirus al 100% Servidores y PC

La E.S.E Hospital Manuel Uribe Ángel y sus sedes no podrá tener dentro de la red institucional computadores que no estén cubiertos por un servicio de antivirus, esto para garantizar que no van a ocurrir problemas de virus o de seguridad.

Así, cualquier computador de un proveedor o tercero que se conecte a la red debe garantizar que tiene un software antivirus actualizado para proteger la red de la E.S.E Hospital Manuel Uribe Ángel y sus sedes.

5.10. Creación y Conexión Centros de Cableado

Los nuevos centros de cableado que requieran conectarse al centro de cableado principal tanto en la E.S.E Hospital Manuel Uribe Ángel y sus sedes deben realizarse con fibra óptica si existe el presupuesto requerido. Adicionalmente, se define como contingencia dejar una línea UTP categoría 6E o superior.

5.11. Reporte Mal Uso Recursos Informáticos

Es deber de todo usuario reportar anomalías en el cuidado de equipos e impresoras; por ejemplo, si derraman un líquido o algún alimento, clip o demás elementos sobre algún equipo de cómputo o impresora, se debe desconectar el equipo y llamar inmediatamente a la oficina de Gestión de Informática.

6. RESPONSABILIDADES DEL USUARIO

6.1. Garantizar USB libres de virus

La E.S.E Hospital Manuel Uribe Ángel debe garantizar que los archivos contenidos en medios de almacenamiento como USB que emplea para el transporte de información estén libres de virus informáticos, para ello se escanea los medios extraíbles con el antivirus institucional, si en el proceso de limpieza algún archivo es desinfectado y eliminado, la E.S.E Hospital Manuel Uribe Ángel no se hace responsable ya que prima la seguridad de la información.

Con lo anterior, se garantiza que la USB que provengan de sitios de alto porcentaje de virus como son universidades, cafés Internet y el Hogar donde no existen unas políticas claras y precisas de Antivirus, afecten la red y la información de la E.S.E Hospital Manuel Uribe Ángel y sus sedes.

6.2. Gestión de Contraseñas

Las contraseñas son un aspecto muy importante de la Seguridad de la Información. Una contraseña débil puede dar lugar a accesos no autorizados y/o explotación de recursos de la ESE.

Todos los usuarios, incluyendo personal asistencial, estudiantes, personal administrativo, contratistas y proveedores con acceso a sistemas de información, redes de comunicación o información de la ESE, son responsables

de tomar las medidas adecuadas para seleccionar y proteger sus contraseñas. Teniendo como propósito establecer un estándar de uso de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambios.

Se define:

Creación de Contraseñas.

- El Periodo de validez para las contraseñas se establece para que caduquen cada 60 días.
- No se permite la reutilización de hasta las últimas 5 contraseñas, ya usadas.
- La contraseña debe cumplir con los siguientes requisitos de complejidad:
 - Debe tener una longitud mínima de doce caracteres.
 - Deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);
 - Caracteres en mayúsculas (de la A a la Z)
 - Caracteres en minúsculas (de la A a la z)
 - Caracteres números (0,1,2,3,4,5,6,7,8,9)
 - Caracteres símbolos (por ejemplo, +, -, (,),[,],!, \$, #, %, etc.)
- No deben contener los siguientes tipos de palabras:
 - Palabras sencillas en cualquier idioma (palabras de diccionarios);
 - Nombres propios, fechas, lugares o datos de carácter personal;
 - Palabras que estén formadas por caracteres próximos en el teclado;
 - Palabras excesivamente cortas.
- Utilizar herramientas en línea que ayudan con la generación de generación de contraseñas seguras.

<https://www.expressvpn.com/es/password-generator?gclid=EAlaIqObChMlxI2EhdqB6wIVDDiGCh0fzg1KEAAYASA AEgLe1 D BwE>

<https://passwordsgenerator.net/es/>

- No deben contener el nombre de la cuenta del usuario o partes del nombre completo del mismo o que excedan de dos caracteres consecutivos.
- No utilizar contraseñas por defecto o de fábrica que traen los equipos y aplicaciones. Con esta medida evitamos el acceso no autorizado. Esto es especialmente para el acceso a la configuración de ciertos dispositivos como Routers, switches, servidores, etc.

Protección de Contraseñas.

- El número de intentos fallidos de inicio de sesión se establece en cuatro, luego de estos la cuenta de usuario se bloqueará por un minuto.
- El bloqueo de la cuenta y la expiración del mismo, está establecido en un minuto.
- Las contraseñas no deben de compartirse con nadie. Todas las contraseñas deben ser tratadas como sensibles y como Información confidencial de la ESE.
- No escriba ni guarde contraseñas en post-its o papel en cualquier lugar de su oficina.
- No debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.
- Las contraseñas de nivel de sistema (por ejemplo, usuario, root, admin, administrador, cuentas de administrador de aplicaciones, etc.) deben de ser cambiadas al menos cada trimestre.
- Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente y cambiar todas sus contraseñas a la brevedad.

6.3. Contenido de los mensajes Institucionales

Todo mensaje enviado desde la dirección electrónica del usuario es de la total responsabilidad del mismo, aunque no haya sido enviado personalmente por él.

La E.S.E Hospital Manuel Uribe Ángel no se hace responsable por lo que se haga o diga en la suplantación a nombre de una cuenta particular enviado como dominio hospitalmua.com.co

6.4. Custodia Insumos Informáticos y control de energía de monitores y computadores

Es responsabilidad de cada usuario proteger los insumos informáticos asignados bajo su custodia para el desempeño de sus funciones. Mientras el usuario está haciendo uso del equipo, es completamente responsable del mismo. En caso de cualquier falla o desperfecto, debe reportarlo de inmediato al personal encargado en Gestión de Informática. El usuario no debe abandonar, ni alejarse físicamente del computador sin antes bloquear el computador o apagarlo físicamente. Se solicita apagar las pantallas cuando se retire de su puesto de trabajo por más de una (1) hora si su puesto de trabajo está en un lugar de alto tráfico de usuarios y/o pacientes. Se solicita apagar el computador cuando se retire de su puesto de trabajo por más de dos (2) horas si su puesto de trabajo está en un lugar de alto tráfico de usuarios y/o pacientes.

6.5. Custodia Insumos Informáticos para uso exclusivo de actividades laborales

Es responsabilidad de cada usuario proteger los insumos informáticos asignados bajo su custodia para el desempeño de sus funciones. Por lo tanto, el uso de la red, el correo y el disco duro de la estación de trabajo es laboral o del ámbito de la salud. No se permite acceder a páginas de Internet que no tienen ámbito laboral, descargar en su estación de trabajo música, juegos, archivos personales y/o académicos, fotos o software free no autorizado por la oficina de Gestión de Informática. Se informa a los usuarios que E.S.E Hospital Manuel Uribe Ángel y sus sedes cuenta con herramientas de gestión de monitoreo automatizadas en línea para el cumplimiento de esta política lo que reporta el uso de Internet de los usuarios. Por lo tanto, cualquier uso no autorizado será notificado directamente por el analista de soporte técnico de la institución.

6.6. Garantizar Legalidad del Software en el equipo asignado

El software disponible en cada computador es propiedad de la E.S.E Hospital Manuel Uribe Ángel, cada usuario es responsable del computador y debe firmar la aceptación de lo instalado en su equipo, si aparece instalado software que no pertenece al Hospital debe reportarlo inmediatamente a sistemas, el usuario es responsable de la legalidad del mismo ante las directivas la E.S.E Hospital Manuel Uribe Ángel, y ante las autoridades externas que realicen la inspección.

Si el computador es compartido todos los usuarios del mismo son responsables del mismo, sin importar quien realizó una instalación indebida.

6.7. No atentar contra insumo informático

En caso que algún usuario dañe o atente contra el buen funcionamiento de algún equipo voluntariamente, tendrá la obligación de cubrir el costo de la reparación, o bien encargarse personalmente de la reparación del insumo informático.

6.8. Responsabilidad de las Copias de Seguridad

El área de Gestión de Informática es responsable de los backup de las unidades de almacenamiento asignadas a cada usuario, la información local de cada equipo es responsabilidad del usuario. Como las cuotas de espacio duro en disco son limitadas, el backup que se envía al servidor son de documentos estrictamente requeridos como un backup especial. Es responsabilidad del usuario realizar backup en CD de otra información de los archivos de las herramientas de trabajo de Office que no se guarde en el servidor como también depurar periódicamente la carpeta definida para el backup para no entorpecer las labores de backup institucionales.

6.9. Notificar anomalías en el cuidado insumos informáticos

Es deber de todo usuario reportar anomalías en el cuidado de equipos e impresoras; por ejemplo, si derraman un líquido o algún alimento sobre algún equipo, se debe desconectar el equipo y llamar inmediatamente a sistemas.

7. ACTIVIDADES NO AUTORIZADAS AL USUARIO

7.1. Manipulación de Información

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario agregar, suprimir o modificar información en carpetas ajenas sin el consentimiento del propietario o por medio de autorización del Jefe de Gestión Informática o el Jefe Inmediato responsable de la información.

7.2. Mensajes Públicos

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario el uso de lenguaje inapropiado u ofensivo, en mensajes privados o públicos.

7.3. Recursos Informáticos para Actividades Personales

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario el uso de los servicios de tecnología para negocios particulares o para actividades no relacionadas con la salud o labores administrativas, ni para el beneficio particular de terceras personas o de instituciones que no tengan autorización o acuerdos con la institución. En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario el uso del computador para grabar, ver u obtener archivos de videos de páginas pornográficas o delictivas o para bajar o grabar música, realizar conexión a páginas no autorizadas, o instalar programas para un fin personal.

7.4. Exceder Cuota Buzón de Mensajes

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario exceder la cuota del Buzón de mensajes con archivos que excedan los 5 megas por correo, las políticas de tamaño de los correos y el buzón de mensajes garantizan el correcto funcionamiento del servicio de mensajería.

7.5. Envío Mensajes no Institucionales

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario enviar a sus compañeros mensajes no institucionales como Chistes, Cuentos, Novelas, presentaciones en PowerPoint de mensajes, Poemas,

Cadenas de Mensajes religiosos, Cadenas de Mensajes de eventos catastróficos y demás que no hayan sido previamente validados que son mensajes verídicos y que aportan al desempeño de las labores institucionales.

Se informa a los usuarios que la En la E.S.E Hospital Manuel Uribe Ángel cuenta con herramientas automatizadas de gestión de monitoreo en línea para el cumplimiento de esta política lo que reporta un filtro de mensajes no institucionales y que se clasifican como SPAM.

Cualquier uso no autorizado será notificado directamente por el analista de soporte técnico de la institución quien tiene la autonomía de determinar si elimina el mensaje y no permite su distribución a sus destinatarios. Igualmente, mensajes con algunas palabras y/o contenidos en ingles o con palabras definidas como SPAM de manera automática por la herramienta de Antivirus, deberán previamente ser filtradas por el Analista de Soporte técnico lo que puede generar que algunos mensajes no lleguen al destinatario del mensaje.

En la E.S.E Hospital Manuel Uribe Ángel no está autorizado al usuario prestar su buzón de correo a terceros no autorizados para utilización de los servicios de mensajería para propósitos no laborales o para la propagación de mensajes destructivos u obscenos, o para enviar correos masivos o spam.

7.6. Red Exclusiva para propósitos laborales

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario prestar su estación de trabajo o punto de red a terceros no autorizados para utilización de los servicios de la red para propósitos no laborales o usarlos para propósitos fraudulentos, comerciales o publicitarios. No está autorizado prestar su punto de red para conectar un PC de un tercero no autorizado por el área de Gestión de Informática o para la conexión de PC personales para bajar información de la red o para realización de actividades personales con portátiles no matriculados como autorizados para conectarse a la Red de la E.S.E.

7.7. Ingreso Personal no autorizado a la Oficina de Gestión de Informática y/o Centro de Cómputo

En la E.S.E Hospital Manuel Uribe Ángel no está autorizado al usuario del área de Gestión de Informática a permitir el ingreso en horario no hábil de lunes a domingo de un tercero o personal de otra área no autorizado por escrito por parte del Jefe Gestión de Informática.

7.8. Cambio Configuración estación de trabajo

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario modificar la configuración de los equipos, adicionar o cambiar puertos, modificar configuraciones, cambiar papel tapiz, descansar pantallas o cualquier otro ítem de configuración sin el consentimiento del personal de soporte técnico del área Gestión de Informática.

7.9. Mover físicamente los insumos informáticos del puesto de trabajo

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario el mover físicamente los equipos de cómputo, impresoras, equipos de red, servidores. Las actividades de movimiento y/o traslado de insumos de informático son labores exclusivas de los analistas de soporte de Gestión de Informática, Cualquier otra persona que lo haga sin la autorización pertinente será directamente responsable de la integridad de los equipos transportados.

7.10. Uso de recursos informáticos en horario no laboral según el cargo

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario el acceso a los servicios informáticos en horario diferente al laboral de lunes a domingo para realizar trabajos diferentes a los asignados al cargo.

7.11. Uso de objetos no acordes a la función del insumo informático

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario poner encima o tener cerca del equipo líquidos, alimentos, papelería pasada, u obstruir la ventilación de los equipos con cualquier objeto, o colocar los insumos de cómputo en el piso donde exista la posibilidad de golpes o maltrato por obstaculizar el paso.

7.12. Intercambio de insumos informáticos que alteren el Inventario de Hardware

En la E.S.E Hospital Manuel Uribe Ángel y sus sedes no está autorizado al usuario o al jefe del usuario intercambiar teclados, CPUS, monitores, reguladores, UPS o impresoras sin la autorización personal de soporte de Gestión de Informática y el personal de Activos Fijos de la E.S.E, estos movimientos alteran el inventario de hardware.

8. REGLAMENTACIÓN PARA NO USUARIOS DE LA En la E.S.E Hospital Manuel Uribe Ángel y sus sedes.

Se deja de ser usuario de los servicios informáticos automáticamente en los siguientes casos:

- Empleados retirados voluntaria e involuntariamente.
- Al terminar el convenio o prácticas en la institución.
- Al terminar outsourcing u ofertas mercantiles de servicios con terceros.
- Por alguna sanción o investigación establecida por las autoridades la E.S.E Hospital Manuel Uribe Ángel o externas.
- Por terminación de cualquier vínculo con la E.S.E Hospital Manuel Uribe Ángel.

9. FALTAS CON TRÁMITE DISCIPLINARIO

- Todo aquel usuario que use una cuenta o use una clave que no le corresponde.
- Facilitar, prestar, alquilar o vender a otra persona su clave(s) personal (password).
- Apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario, grabar o copiar información en carpetas de otros usuarios sin el consentimiento del dueño de la información.
- Perturbar el trabajo de los demás enviando mensajes continuos que impidan en normal funcionamiento del trabajo.
- Violar o intentar violar los sistemas de seguridad de los equipos internos o externos para dañar o obtener información confidencial.
- Jaquear, escuchar o decodificar el tráfico de la red interna o externa o cualquier intento de obtención de información confidencial que se transmita a través de la misma.
- Realizar labores propias de los administradores del sistema sin permiso escrito del personal de sistemas.
- Por ninguna causa se permitirá que los usuarios destapen o traten de reparar los equipos. La instalación de tarjetas y otros elementos, así como la reparación de anomalías son llevadas a cabo por personal de sistemas o terceros autorizados, o personal de mantenimiento autorizado por la oficina de sistemas o por la administración del Hospital.
- Por ninguna causa se permitirá el ingreso a la Oficina de Gestión de Informática a terceros que no estén realizando un trabajo exclusivo para la E.S.E Hospital Manuel Uribe Ángel
- Por ninguna causa se permitirá el ingreso de PC personales de contratistas, empleados de la E.S.E Hospital Manuel Uribe Ángel y sus sedes para que sean revisados, formateados o configurados por personal de soporte del área de Gestión de Informática.

10. RESPONSABILIDAD DEL PROVEEDOR DE OUTSOURCING DE TI

El personal de Ti es responsable de velar el cumplimiento del presente reglamento, cualquier falta u omisión de notificación genera sanción al personal encargado.

11. SANCIONES

Las sanciones acerca del incumplimiento de este reglamento sobre el uso de tecnología se realizan según el vínculo de trabajo que se tenga con la persona que realiza la sanción.

11.1. Servidores Públicos

Se notifica a la oficina de control interno disciplinario donde se aplica la ley 734 de 2002.

11.2. Contratistas

La notificación de la sanción es reportada al interventor del contrato.

11.3. Auditores Médicos

La sanción se reporta a la EPS correspondiente.