POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

E.S.E. HOSPITAL DEL PERPETUO SOCORRO

VILLAVIEJA HUILA

OCTUBRE DE 2020

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

INTRODUCCION

La seguridad que s exigen hoy en dia para las tecnologías de la información es cada vez más alta en día para las tecnologías de la información es cada vez más alta y compleja, esto debido al crecimiento que ha tenido el Internet en los últimos días.

La protección de información y bloqueo de intrusos, son tan solo ejemplos de los objetivos a lograr para que la infraestructura informática de una organización sea segura.

La posibilidad de expandir la cobertura de servicios, de interconectar bases de datos y de acercar a los usuarios separados por grandes distancias, ha llevado a la aparición de nuevas amenazas en los sistemas computarizados, si crece la cobertura, crece la vulnerabilidad.

Hoy a hoy, muchas organizaciones gubernamentales y no gubernamentales, desarrollan políticas de seguridad que rigen el uso adecuado de la tecnología y hacen recomendaciones para aprovechar sus ventajas y evitar su uso indebido; previendo así problemas en el uso de los bienes y servicios informáticos de las entidades.

Las políticas de seguridad informática surgen como una herramienta organizacional necesaria para concientizar a cada uno de los integrantes de una empresa sobre la importancia, la sensibilidad de la información y la necesidad de su conservación con el mínimo de riesgo y un alto grado de seguridad que favorezca el desarrollo de la organización, garantice su óptimo funcionamiento y el buen uso de los equipos y recuperación de la información en el menor tiempo posible en caso de incidentes o eventos catastróficos.

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

1. GLOSARIO

Activo: Conjunto de bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar (manejar o controlar) equipos informáticos o servicios físicamente separados.

Amenaza: Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.

Antivirus: Son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos.

Área Crítica: Área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la Institución.
Bases de Datos: Conjunto de datos interrelacionados y de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

CD (Disco compacto): Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).

Comando: Instrucción u orden que el usuario proporciona a un sistema informático, a través de una línea de texto basada en palabras clave.

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

Dirección IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, una interface de conexión de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).

DVD (Disco Versátil Digital): Dispositivo de almacenamiento óptico en forma de disco, similar al CD, pero de mayor capacidad de almacenamiento (4.7 GB).

Equipo de Cómputo: Dispositivo con la capacidad de aceptar y procesar información, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

Equipo de Telecomunicaciones: Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Estabilizador: Dispositivo para la toma de la tensión dela red eléctrica que alimenta al computador y a la red.

Filtro de contenidos web: Herramienta informática que bloquea o permite el acceso a determinados sitios de internet.

FTP (File Transfer Protocol): Protocolo y software que permite la transferencia de archivos entre máquinas conectadas a una red.

Hardware: Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Integridad: Proteger la información de alteraciones no autorizadas por la institución.

Internet: Red de redes de computadoras conectadas a nivel mundial, se emplea para el intercambio de información, el acceso a bases de datos, entre otros fines.

Mantenimiento: Acciones que tienen como objetivo mantener un artículo o restaurarlo a un estado original.

Memoria USB: Dispositivo de almacenamiento masivo que utiliza memoria flash para guardar la información que se puede requerir. Módulo: Parte de un programa de computador.

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

Red: Conjunto de computadoras y elementos interconectados que permiten una comunicación entre sí y forman parte de un mismo ambiente.

Servicio: Conjunto de aplicativos, programas informáticos o sitios web que apoyan la labor administrativa de la institución, sobre los procesos diarios que demanden información o comunicación en la misma.

Software: Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Software espía: Controla el uso de la computadora sin el conocimiento o consentimiento del usuario. Los softwares espía pueden grabar la secuencia de pulsación de teclas, el historial de navegación, contraseñas y cualquier otra información confidencial y privada, y enviar estos datos a un tercero vía Internet.

Soporte Técnico: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores o equipo de oficina dentro de la institución.

Ups (Uninterrupted Power System): Sistema de Potencia Ininterrumpida, es un dispositivo que, gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

Usuario: Cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga algún tipo de vinculación con la ESE.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ESE Hospital del Perpetuo Socorro de Villavieja Huila, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de estándares, procedimientos, formatos que permitan establecer marco de confianza basados en la seguridad de la información ejerciendo nuestros sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad

3. ALCANCE

La aplicación de estas Políticas de Seguridad Informática, de la ESE Hospital del Perpetuo Socorro de Villavieja Huila, acogería a todos los funcionarios de planta y

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

contratistas, asistenciales y administrativos que hagan uso de herramientas informáticas y/o estén conectados a la red de la institución.

La Política de Seguridad requiere un alto compromiso por parte de cada uno de los funcionarios de la institución, capacidad para detectar fallas y anomalías y el establecimiento de controles continuos para renovar y actualizar dicha política en función del ambiente dinámico, cambiante y evolutivo que nos rodea.

4. OBJETIVO GENERAL

Elaborar las Políticas de Seguridad Informática para ESE Hospital del Perpetuo Socorro de Villavieja Huila, que cree una cultura organizacional de buenas prácticas en el aspecto computacional y fortalecer la protección física y lógica de los activos informáticos de la entidad.

4.1. OBJETIVOS ESPECIFICOS

a) Establecer normas de cuidado de equipos, periféricos y demás dispositivos físicos.
b) Sensibilizar a todos los usuarios de la ESE Hospital del Perpetuo Socorro de Villavieja Huila acerca de la necesidad de poner en práctica dicha Política.
c) Crear mecanismos de protección a partir de la toma de precauciones, básicas pero fundamentales a la hora de utilizar los recursos de red tales como internet o intranet.
d) Reglamentar y controlar la instalación de todo tipo de software, entre todos los funcionarios y contratistas de la ESE Hospital del Perpetuo Socorro de Villavieja Huila
e) Documentar las políticas de seguridad, creadas para la ESE Hospital del Perpetuo Socorro de Villavieja Huila y junto con el plan de contingencia, establecer los parámetros fundamentales de estabilidad y confiabilidad del área informática de la institución.
f) Apoyar la innovación tecnológica.
g) Proteger los activos tecnológicos

5. RIESGOS INFORMÁTICOS

La ISO 27001 (Organización Internacional de Estandarización) define el riesgo informático como: “La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños.”

En una entidad, los riesgos informáticos, son latentes día a día y pueden afectar

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

gravemente la seguridad y la estabilidad de los sistemas de información, estos pueden presentarse en diversas áreas así:

RIESGO INTERNO	RIESGO EXTERNO
Origen Tecnológico: Cuando la infraestructura informática o los mecanismos de protección de la institución fallan. Ej. Caída inesperada de alguno de los servidores, cambios bruscos en el fluido eléctrico de la institución	Origen Tecnológico: Cuando parte de la infraestructura tecnológica de la institución depende de terceros y esta falla inesperadamente. Ej. Caída de la conexión a internet.
Origen Humano: Cuando los usuarios cometen errores (voluntarios o no) al utilizar los recursos informáticos de la institución. Errores en el diligenciamiento de información por parte de los usuarios de la red de la institución, mal manejo de los equipos, pueden causar serias inconsistencias en el sistema.	Origen Humano: Producidos por errores en el suministro de información a la entidad, o errores en soportes técnicos realizados a equipos de la institución por terceros. O también producidos por posibles ataques de hackers desde el exterior. Origen Natural: Cuando eventos extraordinarios de origen natural, afectan físicamente la infraestructura de la institución, tocando también a las redes y equipos informáticos. Ej. Terremotos, incendios, etc.

Para La ESE Hospital del Perpetuo Socorro de Villavieja Huila, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

5.1. POLÍTICAS DE SEGURIDAD

Son las reglas y procedimientos que regulan la forma en que una organización mitiga los riesgos y busca establecer los estándares de seguridad a ser seguidos por todos los involucrados en el uso y mantenimiento de las herramientas tecnológicas.

Se consideran como el primer paso para aumentar la conciencia de seguridad de la información, están orientadas hacia la formación de buenos hábitos.

6. CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Para efectos de comprensión y estructuración de este documento, la oficina de Sistemas de la ESE Hospital del Perpetuo Socorro de Villavieja Huila, ha clasificado las políticas de seguridad en los siguientes grupos:

- Equipos: Todo lo relacionado con el hardware, su uso y cuidado.
- Usuarios: Concerniente a las personas que utilizan los recursos informáticos de la institución
- Software: los recursos lógicos tales como programas, aplicativos y demás.
- Redes e Internet: las medidas que se deben tomar a la hora de utilizar los recursos de telecomunicación.
- Datos e Información: Políticas que regulan la manipulación, transporte y almacenamiento de la información de la institución.
- Administración de seguridad Informática: Establece la forma en que la Oficina de Sistemas de Información gestiona la seguridad de la infraestructura informática de la Institución.

6.1. POLITICAS DE SEGURIDAD DE EQUIPOS

La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: “Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos públicos de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cual quiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.” Los equipos son la parte fundamental para el almacenamiento y gestión de la información. La función de la Oficina de Sistemas de Información es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas en caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura informática. Comprende las siguientes políticas:

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

a) Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de la ESE Hospital del Perpetuo Socorro de Villavieja Huila, sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas, de lo contrario no le será permitido conectar su equipo o dispositivo. Para los equipos que no sean propios de la Institución, se debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica y de datos de la institución, ya que esta no se hace responsable de daños físicos o lógicos que puedan sufrirlos equipos o periféricos de terceros.

b) La oficina de Almacén, tendrá registro de todos los equipos que son propiedad de la ESE Hospital del Perpetuo Socorro de Villavieja Huila, si se requiere hacer un traslado de computador, periférico o accesorio, debe contar con el consentimiento de la oficina de tesorería y del Área de Almacén. Si el equipo necesita trasladarse en calidad de préstamo (periodos de horas o días), debe notificarse a la oficina de tesorería para diligenciar el formato correspondiente.

c) Cualquier equipo, periférico o accesorio de propiedad de la Institución que necesite ser retirado de la Institución tendrá que autorizarlo la Oficina de tesorería con previa información al área de almacén.

d) Todo equipo de la Institución, debe estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse. Todos los equipos, periféricos y accesorios computacionales de la red de la Institución deben estar lejos de dos factores principales: La luz directa del Sol y de humedades, filtraciones y demás medios que puedan hacer que el equipo tenga contacto con el agua.

e) Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original. Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa de la oficina de Tesorería, que evaluará la viabilidad de dicho cambio.

f) La protección física y la limpieza externa de los equipos corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de almacén de la ESE Hospital del Perpetuo Socorro de Villavieja Huila. Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás. En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente a la oficina de tesorería para que coordine el

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

mantenimiento necesario he informará a quien corresponda para que se tomen las medidas correctivas necesarias.

g) Toda instalación de equipo, mantenimiento o proceso de soporte técnico a nivel de hardware, sin importar su nivel de complejidad, debe ser única y exclusivamente realizado por personal que autorice la oficina de tesorería de la ESE Hospital del Perpetuo Socorro de Villavieja Huila.

h) Para solicitar servicio de mantenimiento a un equipo, periférico o accesorio, se debe diligenciar el formato pertinente.

i) El funcionario que cumple funciones de almacenista de la ESE Hospital del Perpetuo Socorro de Villavieja Huila es el único autorizado para manejar, mantener y velar por la integridad y seguridad del servidor, a su vez de mantener las claves de estos.

j) El servidor central de la red de la Institución debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la institución, y con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.

k) Los equipos propiedad de la ESE deben usarse solamente para las actividades propias de Institución, por lo tanto, los usuarios no deben usarlos para asuntos personales. (Delito contra los bienes de la administración pública).

l) Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo.

m) La Oficina de sistemas de la institución debe crear la Hoja d vida de cada equipo tecnológico con el fin de conocer su historial y tener la base de datos de él.

6.2. POLITICAS DE SEGURIDAD DE USUARIOS TECNOLOGICOS

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas establece normas que buscan reducirlos riesgos a la información o infraestructura informática.

Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática. Todos los funcionarios y contratistas de la ESE Hospital del Perpetuo Socorro de Villavieja Huila, deberán cumplir con estos requerimientos de seguridad de la Información.

Igualmente, durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por el Institución.

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

La información almacenada en los equipos de cómputo del ESE Hospital del Perpetuo Socorro de Villavieja Huila y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.
No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Toda información en formato electrónico o impreso de la ESE debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación, con esto se alimenta el inventario y clasificación de los archivos de información.

Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

Procedimiento frente a claves y programas:

1. Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos.

Estos permisos se conceden a solicitud escrita del Tesorero quien debe velar por su adecuado manejo.

2. El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas.

3. Informar inmediatamente a la oficina de Tesorería cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente, en el formato utilizado por la institución.

6.3. POLITICA DE SEGURDAD DE SOFTWARE

1. La gerencia es la única responsable de la instalación de software informático y de telecomunicaciones.
2. En los equipos de cómputo de la Institución, no se permite la instalación de software que no cuente con el licenciamiento apropiado.

Está prohibido el uso de aplicaciones ilegales y el uso de “Keygens” y demás aplicativos.

3. Está totalmente prohibido la instalación de juegos, programas de mensajería o

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

aplicativos que no estén relacionados con las labores institucionales que se realizan en la ESE.

4. Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

5. Las medidas de protección (a nivel de software) son responsabilidad del personal de sistemas y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Tesorería.

6. La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas y a la disponibilidad presupuestal con el que se cuente.

7. Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de Tesorería sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.

6.4. POLITICAS DE SEGURIDAD DE LA RED E INTERNET

1. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de la ESE Hospital del Perpetuo Socorro de Villavieja Huila previa solicitud por escrito.

2. Se prohíbe utilizar la red y los equipos de la ESE para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular

3. Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad: Se prohíbe: Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás. Utilizar los recursos de la ESE Hospital del Perpetuo Socorro de Villavieja Huila para el acceso no autorizado a redes y sistemas remotos.

4. La oficina de Sistemas de tiene habilitado en unos equipos acceso total a internet, con previa autorización de la subgerencia en gestión administrativa y financiera. La oficina de

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

Sistemas de Información no se responsabiliza por pérdidas de información en dicho equipo, La oficina de sistemas realizará monitoreo permanente de tiempos de navegación y actividades realizadas a páginas vistas por parte de los funcionarios y/o contratistas.

5. Los servicios bancarios vía web a nombre de la ESE Hospital del Perpetuo Socorro de Villavieja Huila solamente podrán ser utilizados por el Gerente y Tesorero y únicamente en el equipo que este tenga asignado.

6. Los usos de carpetas compartidas serán administrados por el área de sistemas y con documentos en PDF para que no se han modificadas.

7. Para posibilitar el uso compartido de archivos, la oficina de tesorería tiene habilitado un servidor -- el cual se pueden almacenar y compartir la información Pública y Privada de cada dependencia.

La información Pública puede ser accedida por cualquier funcionario de cualquier dependencia.

La información Privada solo está disponible para los funcionarios de la misma dependencia.

7. PROHIBICIONES

- Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.
- Utilizar los recursos de la ESE para el acceso no autorizado a redes y sistemas remotos.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.
- Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.
- Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.
- Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es

juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.

- El intercambio no autorizado de información de propiedad de la Institución, de

FREDDY ORLANDO BARRAGAN ALVAREZ
Gerente

Carrera 3 No. 3-17
Cel: 321 921 1928
e-mail: esevillavieja@yahoo.es