SALUD
SECRETARÍA DE SALUD

INSTITUTO NACIONAL DE GERIATRÍA
POR UN ENVEJECIMIENTO SANO Y ACTIVO

Subdirección de Administración

Departamento de Informática

Políticas de Seguridad

Blvd. Adolfo Ruiz Cortines No. 2767, Col San Jerónimo Lídice, C.P. 10200, Delegación La Magdalena Contreras, México D.F.
Tel. (55) 5573 8686 **www. geriatria.salud.gob.mx**

Políticas de Seguridad

1.- Seguridad Organizacional

2.- Seguridad Lógica

3.- Uso de Internet

4.- Políticas de Soporte

5.- Políticas de uso del servicio de Telefonía

6.- Glosario

Anexos:

Anexo "a".- Requerimientos mínimos de seguridad

1. Seguridad Organizacional

1.2 Políticas de seguridad.

Art. 1. Todos los activos de hardware, software y recursos en materia de Tecnologías de la Información y Comunicaciones (TIC) son propiedad del Instituto Nacional de Geriatría, de igual forma lo es la información generada y procesada al interior del mismo.

Art. 2. Los servicios de red, comunicación institucional (telefonía) y soporte técnico son de uso exclusivo para el personal del Instituto Nacional de Geriatría (INGER).

Art. 3. El uso de los recursos y servicios de los bienes informáticos son para los fines que convengan al INGER, siendo éstos una herramienta de apoyo para que los usuarios puedan llevar acabo sus funciones, no así para el uso personal o actividad que no sea parte del quehacer institucional.

Art. 4. El Departamento de Informática es el único facultado para realizar cambios, administrar, monitorear y otorgar mantenimiento preventivo o correctivo a los servicios, sistemas y todo lo relativo a TIC'S en la red del INGER.

Art. 5. Los usuarios tendrán acceso a los servicios de red e internet, siempre y cuando se cumplan los requisitos mínimos de seguridad (anexo *a*), y se acaten las disposiciones de conectividad del Departamento de Informática.

Art. 6. La prioridad del INGER es la seguridad de sus activos informáticos, por lo cual el acceso a la red institucional e internet estará sujeto a un análisis de los requerimientos de quien lo solicite, así mismo de no justificarse dicha petición no se otorgará el servicio, o se proveerá con perfil mínimo, de tal forma que no se comprometa la seguridad de la red del INGER.

1.2.1 Responsabilidades por los activos.

Art. 7. Los usuarios son responsables por los activos físicos (hardware), activos de información (bases de datos, archivos, licencias y configuraciones) y activos de software que se les asignen.

Art. 8. Todos los activos de información deberán ser creados, manipulados y resguardados en los equipos y red del INGER.

Art. 9. La información procesada, manipulada o almacenada por los usuarios en los equipos asignados es propiedad del INGER, salvo que de conformidad con las políticas de la Secretaría de Salud y el Gobierno

Federal, así como previa aprobación del Director General del INGER, se acuerde y registre formalmente lo contrario.

Art. 10. La seguridad de la información almacenada en cada equipo es responsabilidad del usuario, así mismo es función del Departamento de Informática proteger ésta información de vulnerabilidades externas a la red institucional.

1.3 Normas de seguridad informática.

1.3.1. En cuanto a políticas generales de seguridad.

Art. 11. El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos de la red institucional de conformidad con la normatividad vigente.

Art. 12. El soporte técnico, servicios de red y asesoría son exclusivos de los equipos del INGER, quedan exentos los equipos de terceros, externos y personales.

Art. 13. Se prestarán servicios de red a externos del INGER, siempre que esto no comprometa la seguridad de la red, exista disponibilidad del servicio, se realice la solicitud formalmente al Departamento de informática por medio oficio anexando justificación.

Art. 14. Los servicios de red y soporte técnico estarán estrictamente restringidos a terceros.

Art. 15. El Departamento de Informática planificará periódicamente mantenimiento preventivo de los equipos, aplicará mantenimiento correctivo a los mismos en caso de ser necesario y otorgará soporte a los usuarios.

Art. 16. El Departamento de Informática hará respaldos periódicos de la información así como la depuración de los discos duros.

Art. 17. El Departamento de Informática realizará respaldos periódicos de los activos de información concentrados en servidores, principalmente de las bases de datos.

Art. 18. El Departamento de Informática, realizará una revisión periódica en los equipos y sistemas con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos informáticos.

Art. 19. El Departamento de Informática revisará el tráfico de paquetes que se estén generando dentro de la red del INGER, a fin de determinar si un usuario o grupo de usuarios está haciendo mal uso de los recursos o se está generando algún problema que pueda llevar a colapsar los servicios de red o de algún sistema.

Art. 20. El administrador de la red, dará de alta y baja a usuarios, esto con apoyo del área de recursos humanos quien deberá proveer de una lista de trabajadores del INGER actualizada.

Art. 21. El Departamento de Informática recomendará sobre el uso e implementación de nuevas tecnologías para la administración de los sistemas y la red.

Art. 22. El Departamento de Informática reportará a la autoridad correspondiente del INGER, sobre fallas en el desempeño de la red con el fin de tomar medidas que optimicen el funcionamiento de la red.

Art. 23. El administrador de la red de conformidad a la normatividad vigente establecerá el uso de los sistemas y servicios de red (restricciones y permisos de los usuarios).

Art. 24. Se suspenderá los servicios de red e internet a cualquier usuario que los utilice fuera del ámbito de sus funciones estipuladas en su contrato laboral.

2. Seguridad Lógica

2.1 Políticas de Seguridad

2.1.1 Control de acceso a los usuarios de la red

Art. 1. Son usuarios de la red toda persona que cuenta con un contrato laboral con el INGER.

Art. 2. Se asignará una cuenta de usuario para ingresar a la red y los servicios que ésta ofrezca únicamente a los usuarios del INGER.

Art. 3. El acceso a la red y sus servicios por parte de externos está restringido y solo será permisible mediante una solicitud formal y justificación.

Art. 4. Se proporcionará el servicio solicitado por un usuario, únicamente si se cumple el procedimiento de autorización necesaria conforme a la normatividad vigente.

Art. 5. Cada equipo tendrá una contraseña, la longitud mínima de caracteres permisibles en una contraseña se establece en 8, los cuales tendrán una combinación preferentemente alfanumérica, incluida en estos caracteres especiales, así como combinación de mayúsculas y minúsculas.

2.1.2 Responsabilidades del usuario

Art. 6. El usuario es responsable de mantener a salvo su contraseña y del uso que haga de su cuenta de usuario a los sistemas o servicios de la red.

Art. 7. El usuario es responsable de eliminar cualquier posibilidad de indicio que facilite a un usuario ajeno o tercero la obtención de la información resguardada en su equipo así como los servicios de red.

Art. 8. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos del INGER, está obligado a reportarlo inmediatamente al Departamento de Informática.

2.1.3 Seguridad de acceso a externos

Art. 9. El acceso a externos será concedido siempre y cuando se cumplan con los requisitos mínimos de seguridad establecidos así como el cumplimiento de la normatividad vigente por el Departamento de Informática.

Art. 10. Todo usuario externo, estará facultado a utilizar únicamente y exclusivamente el servicio que le fue asignado y acatar las responsabilidades que devengan de la utilización del mismo.

2.1.4 Control de acceso a la red.

Art.11. El acceso a la red interna, se permitirá siempre y cuando se cumplan con los requisitos de seguridad, éste será permitido mediante un mecanismo de autentificación.

Art. 12. Se deberá eliminar cualquier acceso a la red sin previa autentificación o validación del usuario o el equipo implicado en el proceso.

Art. 13. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red será motivo de verificación y tendrá como resultado directo la realización de una revisión de seguridad.

Art. 14. Se registrará todo el acceso a los dispositivos de la red y se llevará un histórico en archivos de registro.

2.1.6 Protección contra software malicioso.

Art. 15. Se adquirirá y utilizará software únicamente con licencia, en el caso de software libre deberá ser aprobado por el Departamento de informática teniendo en consideración la seguridad.

Art. 16. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizado y activa la protección en tiempo real.

2.1.8 Mantenimiento

Art. 17. El mantenimiento de los equipos se coordina a través el Departamento de Informática con el proveedor.

Art. 18. Se deberá de contar con un registro de mantenimiento efectuado en los equipos y cambios realizados desde su ingreso al INGER.

2.2 Normas de seguridad informática.

2.2.1 Control de acceso a los usuarios de red

Art. 19. El acceso a la red y los sistemas informáticos del INGER, es únicamente a través de una cuenta de usuario.

Art. 20. La aprobación de acceso de internet y demás servicios de la red, por parte de externos, está sujeta a las siguientes condiciones:

1. Solicitud y justificación formal mediante oficio por parte de un director o subdirector de área.

2. Cumplir con los requerimientos mínimos de seguridad establecidos en la normatividad vigente.
3. Contar con la disponibilidad de conexión a la red y de los recursos informáticos.
4. Autorización del Departamento de Informática.

Art. 21. El incumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red obliga a la suspensión inmediata de su cuenta de usuario y de los servicios proporcionados hasta nueva autorización del Departamento de Informática y de su superior jerárquico o persona responsable.

2.2.2 Control de acceso a la red

Art. 22. Los mecanismos de autentificación y permisos de acceso a la red, deberán ser revisados periódicamente por el Departamento de Informática.

Art. 23. El personal de soporte a escritorios remotos deberá hacerlo desde un equipo interno de la red del INGER, en ningún momento lo hará desde una red pública al menos que se garantice la privacidad de la conexión, aplicando tanto para el soporte técnico del INGER como del proveedor en turno de los equipos de arrendamiento.

Art. 24. El administrador de la red, verificará que el tráfico de red sea, estrictamente normal, la variación de este sin ninguna razón obvia, pondrá en marcha un análisis de la situación.

2.2.3 Uso del sistema operativo

Art. 25. La configuración del sistema operativo de cualquier activo lógico en materia de TIC es únicamente facultad del grupo de administradores del Departamento de Informática, queda prohibido para los usuarios bajo ninguna circunstancia realizar alguna actividad de configuración o administración de los recursos informáticos.

Art. 26. Las cuentas de administrador son propiedad exclusiva del Departamento de Informática.

Art. 27. Solo el personal del Departamento de Informática está facultado para instalar software en los equipos.

3. Uso de Internet

Internet es una herramienta que el INGER brinda a los usuarios para apoyar el cumplimiento de sus funciones.

De acuerdo con lo anterior, el servicio de internet se debe utilizar para consultar información relacionada con el trabajo que se desempeña de manera cotidiana.

Hay contenido que está explícitamente prohibido por el INGER y que el usuario debe abstenerse de consultar y visitar debido a que atenta contra la seguridad de los activos informáticos. Este contenido está compuesto por páginas pornográficas, violentas, terroristas, anarquistas, sexistas, racistas y fanatismo religioso entre otros, esto debido a que son fuente de virus, spam, malware, phishing, etc.

RECOMENDACIONES GENERALES PARA EL USO DE INTERNET

- No descargue programas ejecutables de Internet. Estos pueden contener códigos maliciosos que atentan contra la Seguridad Informática del INGER.
- No descargue archivos de lugares no confiables pues estos son una fuente importante de virus, páginas de juegos, entretenimiento, P2P (Ares), ventas, etc.
- No divulgue su dirección de correo electrónico institucional en Internet. Esta puede ser usada para envió de correos basura (SPAM).
- Cambie su contraseña de acceso a la red regularmente para evitar ser suplantado.
- No le preste su contraseña a nadie. Recuerde que todo lo que se haga con su usuario y su clave es su responsabilidad.

3.1 NORMAS APLICABLES AL USO DEL INTERNET

Art. 1. El servicio de internet debe ser utilizado como una herramienta de apoyo, que facilite el cumplimiento de las funciones de los usuarios estipuladas en su contrato. Todo uso fuera de este ámbito es causa de revisión por parte del Departamento de Informática y como consecuencia suspensión del servicio.

Art. 2. El uso del internet se considera indebido cuando:

a) Atenta contra la veracidad, integridad y confidencialidad de la información del INGER.
b) Atenta contra la integridad de la infraestructura tecnológica del INGER.
c) Reduce la productividad de los usuarios.
d) Pone en riesgo la disponibilidad de los recursos informáticos.

Art. 3. Descargar cualquier tipo de aplicación instalable está estrictamente prohibido.

Art. 4. El Departamento de Informática utilizará los mecanismos necesarios para restringir el acceso a los sitios de internet no permitidos por el INGER.

Art. 5. Se realizarán revisiones periódicas del uso del internet para obtener estadísticas que permitan localizar anomalías en el servicio y balancear el ancho de banda.

Art. 6. El acceso de internet es solo para usuarios y equipos del INGER.

Art. 7. Para brindar la conectividad al servicio de internet se deberá cumplir con los requerimientos mínimos de seguridad (anexo a) y la normatividad vigente.

Art. 8. El acceso a internet es restrictivo por jerarquías y funciones, teniendo la siguiente división:

a) Acceso libre, exceptuando las páginas restrictivas que el INGER especifique.
b) Acceso restringido. En este nivel todas las páginas de entretenimiento, ventas, etc. que estén fuera del ámbito laboral quedan restringidas.
c) Acceso especifico. En esta categoría se implementaran solo servicios específicos para equipos de uso general.

3.2 EXCEPCIONES

Art. 9. El acceso a internet por parte de externos y terceros se otorgara únicamente si se cumplen los siguientes puntos:

a) Solicitud y justificación formal mediante oficio.
b) Contar con la disponibilidad de conexión a la red y de los recursos informáticos.
c) Cumplir con los requerimientos mínimos de seguridad aplicados a terceros y la normatividad vigente.
d) El usuario externo firme de conformidad de acatar la normatividad vigente.

Art. 10. Para acceder a páginas restringidas el usuario deberá hacer una solicitud al Departamento de Informática de la o las páginas a las cual quiere acceder, incluyendo su respectiva justificación.

4. Políticas de Soporte

Art. 1. El Soporte Técnico a los activos en materia de TIC es facultad del Departamento de Informática.

Art. 2. El Departamento de Informática deberá hacer uso de los recursos disponibles para mantener en buenas condiciones los activos informáticos.

Art. 3. Todos los usuarios del INGER tendrán derecho a recibir soporte técnico por parte del Departamento de Informática, siempre y cuando se aplique a los activos informáticos del INGER.

Art. 4. No se proporcionará soporte técnico a equipos personales, ni ajenos al INGER.

Art. 5. El personal de Informática debe ofrecer asesoría a los usuarios para el correcto uso y funcionamiento de los activos, la asesoría no implica capacitación.

4.1 NORMATIVIDAD DE SOPORTE

Art. 6. El personal de Eknology Solutions es el único que puede intervenir los equipos de cómputo que el mismo arrenda al INGER.

Art. 7. El usuario tiene prohibido intervenir a nivel físico y lógico (hardware y software) el equipo de cómputo que le fue asignado o cualquier otro que sea responsabilidad del INGER en caso de falla.

Art. 8. Es responsabilidad del usuario reportar de manera inmediata al Departamento de Informática cualquier anomalía o falla que presente su equipo.

Art. 9. El Departamento de Informática dará atención y seguimiento a las fallas que los usuarios reporten, siempre que esté en función de las actividades institucionales del INGER.

Art 10. El personal de Informática deberá supervisar las condiciones de los activos informáticos periódicamente.

Art. 11. El Departamento de informática deberá preferentemente aplicar mantenimiento correctivo en caso de ser necesario dentro de las instalaciones del INGER siempre que se cuente con los recursos necesarios para dicha reparación.

Art. 12. En el caso particular de los activos de arrendamiento que requieran mantenimiento correctivo fuera de las instalaciones del INGER deberán abandonar las instalaciones sin contener activos de información, de igual forma se aplica a todo equipo que por falta de condiciones o herramientas no se pueda llevar a cabo su reparación dentro del INGER.

Art. 13. El Departamento de Informática dará seguimiento para una respuesta oportuna de los equipos que requieran mantenimiento correctivo, el tiempo de respuesta estará en función de la disponibilidad de los recursos con los que se cuente y de los tiempos del proveedor en cuestión.

Art. 14. Los tiempos de respuesta para acudir a los servicios y solucionar las fallas dependerán de los recursos disponibles (herramientas, personal, etc.) con los que cuente el Departamento de Informática.

Art. 15. El Departamento de Informática solo reportará un informe concreto y básico del status del servicio si el usuario lo solicita.

Art. 16. Se priorizará en caso de emergencia los servicios que requieran especial atención y que afecte de manera global la función del INGER.

Art. 17. El Departamento de Informática se guarda el derecho de jerarquizar y priorizar la atención de los servicios en caso de emergencia.

Art. 18. El Departamento de Informática solo impartirá capacitación en aspectos específicos de la red que mejoren su uso y comprensión, con el objetivo de mejorar la seguridad y eficiencia de la red.

5. Políticas de uso del servicio de Telefonía

1. **Uso del servicio de telefonía.**
   - **1.1** El servicio de telefonía es para uso exclusivo del personal del INGER.
   - **1.2** El servicio de telefonía es una herramienta de apoyo para optimizar la comunicación al interior del INGER.
   - **1.3** La comunicación del interior al exterior y viceversa debe ser con fines que convengan al Instituto, que formen parte de las funciones operativas del mismo, así como de quien utilice el servicio, quien debe apegarse a sus funciones definidas en el Manual de Organización del INGER.
   - **1.4** El servicio de telefonía es restrictivo por jerarquía e importancia de funciones. Teniendo la siguiente estructura:
     a) Dirección General: Telefonía Local, Móvil y LADA Internacional.
     b) Dirección de Área: Telefonía Local, Móvil y LADA Internacional.
     c) Subdirección de Área: Telefonía Local.
     d) Unidad Departamental: Telefonía Local.
     e) Áreas Comunes: Telefonía Local.
   - **1.5** El servicio no es para fines personales o tareas que no formen parte del quehacer diario del INGER.

2. **Responsabilidades del servicio y equipos.**
   - **2.1** Los aparatos telefónicos son propiedad de la empresa TESECOM.
   - **2.2** Los aparatos telefónicos son responsabilidad del INGER y del usuario a quien le es asignado.
   - **2.3** El uso correcto del aparato es responsabilidad directa del usuario a quien se le asignó el resguardo del equipo.
   - **2.4** Es responsabilidad del usuario comunicar al área de Informática cualquier anomalía en el funcionamiento u estado físico del equipo.
   - **2.5** El área de Informática es responsable de mantener en funcionamiento los aparatos telefónicos, dando aviso de fallas y levantando reportes de servicio a la mesa de ayuda de la TESECOM.

6. Glosario

TIC.- Tecnologías de la Información y Comunicaciones.

Tráfico de red.- fenómeno producido cuando a la red (o parte de ella) se le ofrece más tráfico del que puede soportar.

IP.- Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

P2P.- red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Spam.- correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Malware.- del inglés malicious software, también llamado código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse y dañar una computadora.

Phishing.- término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Firewall.- Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Usuario. Toda persona que cuenta con un contrato laboral con el Instituto Nacional de Geriatría, realice alguna actividad institucional y previa autorización de uso a los recursos en materia de TIC con los que cuenta el Instituto Nacional de Geriatría.

Administrador. Persona del Departamento de Informática previamente autorizada por el mando superior jerárquico del área de Informática para administrar los recursos informáticos del Instituto Nacional de Geriatría.

Facultades del Administrador:

1. En la red Local:

a) Implementación, configuración, mantenimiento y supervisión de los elementos físicos (switch, routers, servidores, etc.) y lógicos (reglas de ruteo, permisos, etc.) de la red local y la comunicación con otra red.
b) Asignación de direcciones IP de los elementos de la red.
e) Asignación de tablas de ruteo.
d) Implementación de medidas de seguridad para la red.
e) configuración de autentificación y autorización a la red.

2. En los servicios:
a) Configuración de autentificación y autorización de los servicios de la red .
b) Configuración de los servicios.
e) Monitoreo y supervisión de los servicios.

3. Bases de datos:
a) Implementación, configuración, mantenimiento, supervisión, respaldo y resguardo de las Bases de Datos.
b) Configuración de autentificación y autorización a las Bases de Datos.
e) Control sobre las Bases de Datos (Escritura, borrado, modificación, etc.).
d) Asignación de permisos sobre las bases de datos.
e) Implementación de medidas de seguridad de acceso a las Bases de Datos.

4. Sistemas Desarrollados y Sistemas Operativos:
a) Configurar, modificar y supervisar los sistemas.
b) Intervenir y dar mantenimiento preventivo y correctivo a nivel lógico de los sistemas.
e) Instalar software y hardware.
d) Otorgar permisos de uso y acceso a los sistemas.
e) Alterar la configuración de otros usuarios.

De lo anterior se desprende que existen los siguientes usuarios con privilegios de administrador:
1. Administrador de red.
2. Administrador de bases de datos.
3. Administrador de respaldos.
4. Administrador de servicios de publicación.
5. Administrador de servicios de red.

Externo. Toda persona que mantenga una relación de colaboración con el Instituto Nacional de Geriatría, realice actividades institucionales dentro de sus instalaciones pero que no cuenta con un contrato laboral con el Instituto Nacional de Geriatría.

Terceros. Toda persona que no guarde una relación directa con el Instituto Nacional de Geriatría, ingrese a sus instalaciones en calidad de visitante.

ANEXO "A"

REQUERIMIENTOS MÍNIMOS DE SEGURIDAD QUE SE DEBEN CUMPLIR PARA INGRESAR A LA RED INTERNA DEL INSTITUTO NACIONAL DE GERIATRIA (INGER).

Requerimientos para usuarios del INGER

1. Todo usuario que deseé ingresar a la red del INGER deberá contar con un nombre de usuario y contraseña. El usuario y contraseña son personales, no deben ser difundidos o transferidos.
2. Ningún usuario puede contar con privilegios de administrador sobre el sistema operativo o cualquier servicio de la red.
3. El Departamento de Informática es el responsable de configurar y modificar el sistema operativo, los servicios de red o cualquier sistema que así lo requiera.
4. Las cuentas con privilegios de administrador son de uso exclusivo del Departamento de Informática.
5. Los equipos que se integren a la red deberán cumplir con:
    a. El software instalado en los equipos debe de ser únicamente el sistema operativo y el software institucional. Todo el software debe contar con licencia.
    b. Sistema operativo actualizado.
    c. El sistema operativo se debe configurar, para evitar anomalías en el sistema, virus o intrusiones externas.
    d. Antivirus institucional con licencia, actualizado, configurado y con protección en tiempo real.
    e. No debe contar con ningún software de tipo administrativo, local y de red que modifique o tome control del sistema operativo, así mismo de cualquier servicio de red.

Requerimientos para usuarios externos.

1. Los usuarios externos tendrán acceso a los servicios de red previa autorización del Departamento de informática y bajo la responsabilidad de quien solicite proveer de algún servicio a externos y terceros, de acuerdo a lo establecido en las políticas informáticas del INGER.
2. No se proporcionaran contraseñas de los servicios de red, dominio e internet.

3. Los equipos personales de los usuarios externos que se integren a la red deberán cumplir con:
    a. Sistema Operativo con licencia.
    b. El equipo debe estar libre de virus.
    c. Sistema operativo correctamente configurado, evitando vulnerabilidades del sistema, virus o intrusiones externas.
    d. Suite de Antivirus (spyware, malware, y firewall) con licencia, actualizado, configurado y con protección en tiempo real.
    e. No se prestara el servicio si se tiene instalado algún software del tipo p2p (Torrents, Ares, eMule, eDonkey, Morpheus, etc.) o cualquiera que realice conexiones punto a punto.
    f. No debe contar con ningún software de tipo administrativo, local y de red que modifique o tome control del sistema operativo, así mismo de cualquier servicio de red.
4. El software instalado debe estar correctamente configurado, libre de agujeros o parches que comprometan la seguridad, principalmente en software sin licencia, pirata y libre.
5. El Departamento de Informática monitoreara la actividad de externos y terceros.