

Política de Uso Apropriado de Estaciones de Trabajo (Computadoras)

Efectivo: 14 de abril de 2003

Propósito

Esta política establece las reglas de uso para los recursos de computadoras.

Alcance

Esta política aplica...;

- a todos los miembros de la fuerza labora (empleados, facultad, enfermeras, estudiantes, voluntarios, etc.) del Departamento de Salud, así como contratistas y asociados de negocio se encuentran realizando labores en la facilidades de la organización.
- a toda computadora, programado y/o sistema de comunicación dentro de las facilidades del Departamento de Salud; a todas las plataformas (sistemas operativos) y a todos los programados en uso.
- en combinación con la "Política de Control de Acceso a Sistemas con PHI".

Política

Conceptos Generales

1. El uso de las computadoras del Departamento de Salud deberá se apropiado, legal, ético y cooperativo.
2. El Departamento de Salud, mediante su oficial de Seguridad, tomará decisiones según se ~~ya~~ necesarias para que los usos específicos de las computadoras sean cónsonos con esta política.
3. El Oficial de Seguridad será la autoridad final en el uso de computadoras así como en el otorgamiento de acceso y cuentas.
4. Todos los datos creados y/o guardados en las computadoras del Departamento de Salud se convertirán en propiedad del Departamento de Salud.

Monitoreo de los Sistemas Computarizados

5. El Oficial de Seguridad tiene derecho de monitorear las actividades de las computadoras para asegurar el uso correcto de las mismas para cumplimiento con esta y otras políticas.
6. La información recopilada durante el monitoreo del Oficial de Seguridad podrá ser utilizada como evidencia en acciones disciplinarias o correctivas, o en acciones legales si fuese necesario.

Uso Apropriado

7. Los equipos de Computadora provistos por el Departamento de Salud son para uso exclusivo de operaciones de negocio del Departamento de Salud y no pueden ser utilizados para propósitos ajenos a la misión de la organización.
8. No se permitirán anuncios ni campañas políticas o religiosas en las computadoras del Departamento de Salud.
9. Se prohíbe el uso de computadoras dentro del Departamento de Salud para acceder o propagar material obsceno, pornográfico, profano o de algún modo objetable.
10. Cualquier equipo computarizado ajeno (que no sea propiedad o provisto por el Departamento de Salud conectado a las redes del Departamento de Salud será utilizado conforme el uso que se le da a los equipos provistos por el Departamento de Salud.

Aclaración – Aunque esta política prohíbe el acceso a material inapropiado, los usuarios podrían acceder material ofensivo a través del Internet inadvertidamente. Mediante este aviso los usuarios son notificados sobre su responsabilidad por los sitios que ellos acceden y las repercusiones que esto pueda tener.

Uso Legal

11. Las computadoras no serán utilizadas para ninguna actividad ilegal.
12. Los miembros de la fuerza laboral se regirán por las leyes federales y estatales que regulan el uso de las comunicaciones y las computadoras.
13. El Departamento de Salud considerará las siguientes actividades como "uso ilegal"
 - Acoso de otros usuarios
 - Difamación de algún usuario
 - Destrucción o daños de los equipos, programados o información bajo custodia del Departamento de Salud o algún otro usuario
 - Interrupción o monitoreo sin autorización de las comunicaciones electrónicas
 - Copiar material con derechos reservados sin autorización
 - Guardar en las computadoras del Departamento de Salud información ilegal o ilegalmente adquirida
 - Violaciones a la confidencialidad
 - Violaciones a las licencias de programados
 - Etc.

Uso Ético y Aceptable

14. Las computadoras deberán ser utilizadas de acuerdo con los estándares de ética y misión del Departamento de Salud. Cualquier uso que no cumpla con estas premisas podría considerarse "usos inaceptable" de los recursos del Departamento de Salud.
15. Algunos usos inaceptables pudieran repercutir en consecuencias legales si se viola ley y/o derechos de alguna entidad o persona: en cuyo caso, el usuario pudiera ser responsable y tener que indemnizar por sus acciones o usos al Departamento de Salud.

16. El Departamento de Salud considerará las siguientes actividades como "usos inaceptables":

- Violación del sistema de seguridad de las computadoras
- Violación a las guías de la red de computadoras
- Utilización de cuentas de computadoras, código de accesos o números de identificación en la red pertenecientes otro usuario
- Utilización de computadoras de manera que innecesariamente impida el funcionamiento o labor de otros
- Acceso inapropiado para acceder y/o compartir información de salud del paciente
- Violaciones a las políticas y regulaciones de utilización de la red
- Violación a privacidad de otro usuario
- Etc.

Uso Cooperativo

17. El Departamento de Salud y su fuerza laboral reconocen que los equipos de computadora conectados a la redes de (Nombre de la Entidad Cubierta) son recursos que facilitan las tareas que se llevan a cabo; por lo que su utilización es "cooperativa".

18. El Departamento de Salud solicitará que los miembros de su fuerza laboral ejerzan las siguientes consideraciones en apoyo del espíritu "cooperativo" de sus recursos:

- Uso prudente del servicio de correo electrónico y resguardo prudente de las comunicaciones
- Consideración en el tiempo que se utilizan las computadoras
- Consideración en el espacio utilizado para guardar información
- Consideración en el uso de recursos de impresión
- Consideración la capacidad de procesos de datos de la computadora
- Consideración a los derechos y privilegios de los demás usuarios

19. En situaciones donde varios empleados se encuentran aglomerados alrededor de una pantalla de alguna estación, el empleado encargado del uso de esa estación deberá cerciorarse de que aquellos que se encuentren allí, tengan derecho o acceso a ver dicha información, para que se pueda dar el uso "cooperativo". A su vez, deberá informarse de esa situación al oficial de Seguridad de (Nombre de la Entidad Cubierta)

Uso del Correo Electrónico ("E-mail")

20. El Departamento de Salud y su fuerza laboral reconocen que el uso de correo electrónico no es un medio seguro de comunicación.

21. El Departamento de Salud advertirá sobre la necesidad de tener precaución al dirigir correos a direcciones electrónicas agrupadas.

22. El correo electrónico interno ("Intranet") podrá tener PHI.

23. Correo interno con PHI debe adherirse a lo siguiente.

- El que recibe el comunicado debe tener una necesidad válida para tener acceso a la información.
- La transmisión de PHI debe ser para propósitos de tratamiento, pago u operaciones.
- La distribución de transmisiones se debe limitadas al mínimo de recipientes posible
- Se recomienda e uso de medidas adicionales de seguridad (como cifrado, firmas electrónicas, aviso de confidencialidad, etc.) tan pronto se hagan disponibles.

24. El envío de correo electrónico con PHI hacia el exterior ("Extranet") está prohibido a no ser que se usen medidas de criptografía para proteger su contenido

Contraseñas ("Passwords") y Accesos al Sistema

25. Los usuarios NO deberán hacer público sus cuentas ni contraseñas; **NUNCA, BAJO NINGUNA CIRCUNSTANCIA NI RAZON, DEBERAN SER DIVULGADOS A OTROS.**
26. Los supervisores o gerentes no requerirán a sus subalternos que le divulguen sus contraseñas o alguna otra información sobre sus cuentas de acceso a particulares a menos que estén autorizados para ello por el oficial de Seguridad, el Oficial de Privacidad y la Administración.
27. Las contraseñas, códigos de acceso, códigos secretos, "tokens", nombres de usuarios, así como lo mecanismos utilizados para acceder los sistemas del Departamento de Salud, se tratarán con **información confidencial**.
28. Las contraseñas no deben ser fáciles de adivinar y deberán ser mayores a ocho (8) caracteres
29. Las contraseñas no deberán ser igual al nombre de cuenta o usuario
30. Los usuarios podrán tener más de una cuenta de acceso; dependiendo de sus funciones
31. Los usuarios son responsables por todo el trabajo realizado bajo su cuenta de acceso por lo que:
 - serán responsables de terminar sus sesiones de comunicación (desconectarse) apropiadamente
 - asegurarse que nadie tenga acceso a su cuenta.
32. Los controles de acceso a programados deben ser únicos para confiar en las auditorías de utilización y acceso de los sistemas.
33. Si un usuario tiene razones para pensar que alguien ha utilizado o aprendido su identificación, contraseña o cuenta de acceso, deberá notificarlo inmediatamente a su supervisor, gerente de sistemas o al Oficial de Privacidad; y el asunto se debe atender de inmediato.
34. Los supervisores, gerentes o sus designados, son responsables de notificar cambios requeridos en cuentas de usuarios debido a cambios de nombre, clasificación, requerimientos de trabajo, etc.
35. Cualquier terminación de cuentas debe ser reportada de inmediato para tomar medidas inmediatas.

Visibilidad de Estaciones / Terminales de Trabajo

36. Las estaciones o terminales estarán localizadas de manera tal que la información desplegada en sus pantallas esté protegida de divulgación inadvertida por personas que pasen por éstas y que puedan ver su información.
37. Protectores de Pantallas ("screen savers") deben ser utilizados para proveer seguridad visual adicional.

Programados

38. Solamente programados con licencia y aprobados, revisados e instalados por persona del Departamento de Salud, pueden ser instalados y utilizados en las computadoras provistas por el Departamento de Salud
39. los usuarios no harán copias ilegales de programados de ningún tipo.
40. En adición a medidas disciplinarias del Departamento de Salud, el usuario será responsabilizado por gastos en los que se incurra como resultado de cualquier acción por tal uso ilegal.

Sanciones, Acciones Correctivas y Disciplinarias:

Violaciones a lo establecido en esta Política conllevará sanciones según especificado en la Política de Sanciones y Manual de Medidas disciplinarias del Departamento de Salud.

