SECRETARÍA DE EDUCACIÓN
DURANGO
GOBIERNO DEL ESTADO

INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS
INEA

POLÍTICAS PARA LA SEGURIDAD

DEL EQUIPO DE CÓMPUTO DEL USUARIO FINAL

Marzo de 2014

Ramírez No. 110 Sur, Zona Centro, C.P. 34000, Durango, Dgo.
Tel (618) 811 13 73 / 01800 640 58 25
www.idea.gob.mx

I. PREPARACIÓN DE EQUIPO DE CÓMPUTO PARA SU ENTREGA AL USUARIO

1. Todo equipo de cómputo institucional registrado en la red, deberá contar con el antivirus instalado y actualizado que determine el Departamento de Informática para la prevención, detección y limpia de virus. Queda estrictamente prohibido remover o sustituir el programa institucional para la detección de virus.

2. El Departamento de Informática será el responsable de configurar los perfiles de usuario y nombres de los equipos de cómputo cuando se cambie o agregue un equipo.

3. Con el propósito de estandarizar el uso de programas de cómputo en el Instituto, sólo se deberán utilizar los programas que sean preinstalados por personal técnico del Departamento de Informática en los equipos de cómputo. En el caso de requerir algún software adicional, deberá solicitarse al Departamento de Informática mediante oficio firmado por el Titular del área requirente.

II. ENTREGA DE EQUIPO DE CÓMPUTO AL USUARIO

4. Al momento de la entrega de un equipo de cómputo, el usuario deberá registrar en el equipo su contraseña (password) de acceso. Adicionalmente el Departamento de Informática deberá otorgarle, a todos los usuarios que corresponda, su contraseña de acceso al correo electrónico.

   Para generar una contraseña segura se recomienda mezclar mayúsculas, minúsculas, números y caracteres especiales, con un mínimo de 7 caracteres.

5. Bajo ninguna circunstancia se otorgará la contraseña de la cuenta administrador. Tampoco se otorgarán cuentas con privilegios de administrador a los usuarios.

III. ENCENDIDO DEL EQUIPO DE CÓMPUTO

6. Al iniciar la jornada de trabajo deberá encenderse el equipo de cómputo en el siguiente orden: monitor, impresora (de contar con ella), equipo periférico (escáner, bocinas, etc.) y CPU.

IV. DURANTE LA JORNADA DE TRABAJO

7. El equipo de cómputo institucional se utilizará únicamente para apoyar las funciones, servicios, trámites, procesos o procedimientos inherentes al cargo del usuario.

8. Los discos flexibles, CD's, memorias USB o cualquier medio de almacenamiento de datos auxiliares propiedad del Instituto, deberán permanecer protegidos y libres de contacto de elementos como: polvo, humedad, altas temperaturas y objetos magnéticos.

9. Es responsabilidad del usuario del equipo de cómputo reportar a la Mesa de Servicio (extensión 515) cualquier irregularidad con el programa de antivirus instalado. Queda prohibido utilizar y/o instalar productos alternativos.

10. Todo equipo de cómputo que no cuente con el programa institucional de antivirus, será puesto en cuarentena por el

Departamento de Informática hasta que le sea instalado el antivirus.

11. Sólo se podrán instalar programas de cómputo autorizados y que cuenten con licencia de uso en los equipos de cómputo, quedando prohibido utilizar programas o software “pirata”, ya que éstos pueden contener spyware, virus o archivos de sistema incompatibles que dañen al equipo.

12. Todo aquel responsable de equipo de cómputo que instale en su computadora paquetes de cómputo sin licencia, se hará acreedor a las sanciones legales que hace mención la Ley Federal de Derechos de Autor.

13. Cualquier falla en los equipos y programas de cómputo deberá ser reportada a la Mesa de Servicio, extensión telefónica (extensión 515).

    La autorización de uso de programas de cómputo clasificados como freeware o shareware deberá ser gestionado ante el Departamento de Informática mediante oficio en el cual justifique su uso; y será esta Área la encargada de valorar que existan las condiciones de seguridad para su instalación.

14. Queda prohibido a los usuarios realizar cambios a: dirección IP, máscara de subred, puerta de enlace predeterminada, DNS, sufijos DNS y habilitación de protocolos a equipos de cómputo, servidores y teléfonos. Se debe poner especial cuidado en lo referente a la dirección IP, toda vez que ésta controla los servicios de comunicaciones;
15. El uso de programas, como proxys, que vulneran la configuración de la red quedan altamente prohibidos.

16. El Departamento de Informática definirá el perfil de acceso a Internet de cada usuario, tomando como base su nivel jerárquico.

17. El uso del servicio de Internet será única y exclusivamente para fines laborales. El acceso a material violento, pornográfico, música, chats y en general a aquello que no contribuya a la productividad laboral queda prohibido.

18. El Departamento de Informática se reserva el derecho a monitorear el uso del servicio de Internet, por lo que cualquier infracción al numeral anterior motivará la baja temporal o definitiva del servicio.

19. Es responsabilidad del usuario mantener la confidencialidad de su(s) acceso(s), cuenta(s) y contraseña(s); y de las actividades que se realicen bajo su uso.

20. El servicio de correo electrónico tiene fines estrictamente laborales para el Instituto; por lo que queda prohibido realizar las siguientes acciones:

    a. Encuestas, concursos, listas de distribución, cadenas de mensajes, correo electrónico no deseado, spamming o cualquier otro tipo de mensajes no solicitados ni consentidos (comerciales o de otro tipo).

    b. La transmisión de material pornográfico, chistes, música, cadenas y en general de aquello que no contribuya a la productividad laboral.

    c. Utilizar el servicio de correo electrónico para cualquier propósito que sea ilícito o esté prohibido.

d. Usar el servicio de correo electrónico de modo tal que pueda dañar, deshabilitar, sobrecargar o deteriorar algún sitio o servicio del Instituto (o las redes conectadas a algún sitio o servicio de la Institución).

e. Intentar obtener acceso no autorizado a sitios o servicios del Instituto, a otras cuentas, sistemas informáticos o redes conectadas a algún sitio o servicio mediante actos de intrusión (hacking), descifre de contraseñas (password mining) y/o por cualquier otro medio.

f. Difamar, abusar, acosar, acechar, amenazar o infringir los derechos (tales como la intimidad y la propia imagen) de terceros.

g. Publicar, anunciar, cargar, distribuir o divulgar cualquier asunto, nombre, material o información inapropiados, profanos, difamatorios, obscenos, inmorales o ilícitos.

h. Publicar, anunciar, cargar, distribuir o divulgar cualquier asunto, nombre, material o información que fomente la discriminación, la violencia o el odio hacia una persona o colectividad, por razón de su pertenencia a una raza, religión o nación.

i. Cargar archivos que contengan imágenes, fotografías, software u otro material protegido por las leyes sobre propiedad intelectual e industrial; incluyendo, a modo de ejemplo y no como enumeración cerrada, las leyes sobre derechos de autor y marcas, a menos que el usuario sea titular de los derechos respectivos o haya recibido todos los consentimientos necesarios para hacerlo.

j. Cargar archivos que contengan virus, "caballos de Troya", "gusanos", bombas de tiempo, sistemas de cancelación de exposiciones (cancelbots), archivos dañados, o cualquier otro programa o software similar que pueda perjudicar el funcionamiento del servicio de correo electrónico y la infraestructura informática y de comunicaciones del Instituto.

k. Anunciar u ofrecer la venta o compra de cualquier bien o servicio con fines comerciales no institucionales.

l. Infringir cualquier punto del Código de Conducta para los Servidores Públicos de la Administración Pública Federal.

m. Infringir cualquier ley o normativa aplicable de la Administración Pública Federal.

21. El tamaño máximo de los archivos adjuntos a un correo electrónico será de 10 MB.

22. El Departamento de Informática cancelará de manera inmediata, toda cuenta que transmita o que esté relacionada con el envío de correo electrónico masivo no solicitado o spamming. Realizadas las aclaraciones del caso, la DAS podrá rehabilitar el servicio cancelado.

23. El usuario hará uso de el servicio de correo electrónico, aplicando las siguientes recomendaciones de uso:

a. No adjuntar archivos con extensiones .com .exe .dll u otro tipo de aplicaciones ejecutables, por la alta

probabilidad de que este tipo de archivos contengan virus y/o código malicioso.

b. No adjuntar imágenes digitalizadas con extensión .bmp, toda vez que generan saturación en las cuentas de los usuarios. Se recomienda utilizar extensión .jpg o .tif.

c. Al enviar correos a una lista de distribución propia, deberá asegurarse que ésta contenga a los destinatarios directamente involucrados o interesados a los que se desea hacer llegar el correo.

24. Un virus es un programa no autorizado, el cual se replica y se propaga causando daños. Si el usuario sospecha de la presencia de virus porque su equipo empiece a comportarse fuera de lo normal, es necesario que apague su equipo y reporte de inmediato el incidente a la Mesa de Servicio.

25. El usuario no deberá descargar software de terceros, principalmente de Internet, ya que este software puede contener virus, caballos de troya, gusanos y otro tipo de software que puede dañar el funcionamiento de los equipos de cómputo. En caso de requerir alguna aplicación, deberá primero solicitarla al Departamento de Informática mediante oficio firmado por el Titular del área requirente.

26. El usuario deberá mantener una navegación segura en internet, no abriendo sitios dudosos y evitando dar “clic” en publicidad engañosa.

27. Cuando el usuario se ausente de su escritorio o sitio de trabajo, no deberá mantener sesiones activas en su equipo de cómputo, debiendo abandonar (salirse de) las sesiones de trabajo y cerrar las aplicaciones que este usando; ya que es su responsabilidad las operaciones que se realicen en las aplicaciones que en ese momento mantenga activas, así como el mal uso que se le dé a los códigos de acceso que le fueron asignados.

28. El usuario deberá aceptar las actualizaciones de seguridad que aparezcan en el equipo de cómputo, debiendo permitir que las actualizaciones concluyan.

29. El Departamento de Informática tendrá la responsabilidad de administrar y regular el uso y crecimiento de la red local de voz y datos por lo que el usuario no podrá agregar nodos sin la autorización de ésta, la cual deberá ser solicitada a través del Oficio correspondiente. La resolución estará sujeta a la disponibilidad presupuestal en caso de requerir de la contratación de una empresa externa para su atención.

30. Antes de conectar temporalmente un equipo a la red local, ya sea de personal local o externo, el Departamento de Informática verificará que el equipo de cómputo tenga actualizado su antivirus y las actualizaciones de seguridad del sistema operativo.

31. Por seguridad de la información, las contraseñas deberán cambiarse preferentemente cada 3 meses.

32. El usuario no deberá atender indicaciones o instrucciones, tanto en internet como en el correo electrónico, de emisores no identificados o de dudosa procedencia; ya que puede contener software malicioso, virus, gusanos y/o caballos de troya que pueden dañar el funcionamiento del equipo de cómputo o extraer información. En caso de duda o sospecha, comunicarse a la Mesa de Servicio (extensión 515).

V. APAGADO DEL EQUIPO DE CÓMPUTO

33. Al terminar la jornada de trabajo deberá apagarse el equipo de cómputo en el siguiente orden: CPU, equipo periférico (escáner, bocinas, etc.), impresora (de contar con ella) y monitor.

VI. APLICACIONES INFORMÁTICAS

34. Todo equipo multiusuario (servidor) y equipo de comunicaciones departamentales deben estar instalados en áreas protegidas y con accesos restringidos.

35. Para realizar la liberación de una aplicación, la Dirección o Unidad responsable -con supervisión de personal del Departamento de Informática- deberá realizar pruebas de estrés para garantizar el buen funcionamiento, las cuales deben incluir el aseguramiento de código y ambiente, utilizando las herramientas que la Dirección o Unidad defina para tal efecto.

36. La Dirección o Unidad responsable de una aplicación informática tendrá la obligación de mantener en condiciones óptimas su operatividad, capacitación técnica y mantenimiento lógico de la aplicación.

37. Las áreas deberán respaldar su información crítica de forma periódica en un medio de almacenaje externo al equipo de cómputo, para lo cual deberán recurrir al Departamento de Informática que será la responsable de la administración de los respaldos.

38. Será responsabilidad del Departamento de Informática mantener en condiciones óptimas de operatividad los equipos y medios de comunicación que utilicen las aplicaciones para su correcto funcionamiento, esto se refiere a las condiciones físicas y de seguridad lógica de la información.

39. El mal uso de las cuentas de usuario, así como de las contraseñas de una aplicación informática; será responsabilidad de quien las tenga asignadas; por lo cual deberá evitarse proporcionar las cuentas y contraseñas a terceras personas.

40. Los protocolos de telnet y ftp serán administrados por el Departamento de Informática, debido al riesgo que representan para la seguridad de la red de datos. De ser requeridos servicios en estos rubros, los usuarios deberán solicitarlos mediante oficio dirigido al Departamento de Informática firmado por el Titular del área requirente.

41. El Departamento de Informática se reserva el envío masivo de correos electrónicos; para ésto el usuario deberá enviar al Departamento de Informática por correo electrónico la solicitud correspondiente, adjuntando el mensaje masivo.

42. El Departamento de Informática se reserva el derecho de suspender el acceso al servicio de correo electrónico, internet y al filtrado de contenidos en cualquier momento, cuando se viole cualquier aspecto de seguridad.